Over-The-Top Bypass: Study of a Recent Telephony Fraud

Merve Sahin
Eurecom & Monaco Digital Security Agency
merve.sahin@eurecom.fr

Aurélien Francillon
Eurecom
aurelien.francillon@eurecom.fr

ABSTRACT

In this paper, we study the *Over-The-Top (OTT) bypass* fraud, a recent form of interconnect telecom fraud. In OTT bypass, a normal phone call is diverted over IP to a voice chat application on a smartphone, instead of being terminated over the normal telecom infrastructure. This rerouting (or hijack) is performed by an international transit operator in coordination with the OTT service provider, but without explicit authorization from the caller, callee and their operators. By doing so, they collect a large share of the call charge and induce a significant loss of revenue to the bypassed operators. Moreover, this practice degrades the quality of service without providing any benefits for the users.

In this paper, we study the possible techniques to detect and measure this fraud and evaluate the real impact of OTT bypass on a small European country. For this, we performed more than 15,000 test calls during 8 months and conducted a user study with more than 8,000 users.

In our measurements, we observed up to 83% of calls being subject to OTT bypass. Additionally, we show that OTT bypass degrades the quality of service, and sometimes collide with other fraud schemes, exacerbating the quality issues. Our user study shows that OTT bypass and its effects are poorly understood by users.

1. INTRODUCTION

Telephony networks carry a huge volume of call, messaging and data traffic every day. This is a complex and opaque ecosystem, which combines multiple technologies and involves various types of service providers and customers. The Public Switched Telephone Network (PSTN) has been the primary medium enabling telephony since the last century. Today, the *global telephony network* encompasses many different technologies such as Voice over IP (VoIP) and cellular networks. VoIP technology has become a major part of the global telephony network, e.g., it is used for dedicated peering links between operators or to reach VOIP phones with regular, internationally routable, phone numbers[1]. Because calls can be expensive, and are billed individually, telephony is a very profitable environment for many fraud schemes. The CFCA estimates the global fraud affecting telecom operators to be worth $38.1 Billion in 2015 [6].

So-called *Over-The-Top* (OTT) services (e.g., WhatsApp, Skype) use IP networks to implement a service without involving telecom operators (i.e., passing “over the top” of them). Because of their global presence, through smartphone application markets, OTT providers attract more customers than most telecom operators. Indeed, studies forecast 2 billion users of OTT messaging by 2018 [21]. OTT applications often provide voice communication services, but they are normally not a part of the global telephony network. However, interconnection between OTT and global telephony network is possible through some gateways, which we will explain in Section 2.1.1.

In this work, we present and analyze a recent type of telephony fraud, called *OTT bypass* or *OTT hijack*, which arises from a new kind of interconnection between telephony networks and OTT applications. Indeed, in an OTT bypass the OTT provider partners with a transit operator to hijack regular calls (i.e., calls originated from a mobile or landline phone to a mobile number) to terminate them over the OTT application. The large user base of OTT applications, and the high termination fee of some international destinations, make this practice very profitable for the OTT provider and partnering operators. Indeed, OTT bypass has been reported to cause losses to telecom operators in the order of tens of millions of Dollars [8]. Moreover, users and other operators are affected in many ways, as we will study throughout this paper.

Telephony and OTT regulation.

In order to protect customers, promote competition, and prevent market abuses, telecommunications industries are often subject to strict government regulation [24]. OTT providers are not subject to these regulations, even though they provide similar services. There are efforts to regulate OTTs and VoIP services in some countries [11, 44], but this remain a challenge. A common argument is that OTTs are fundamentally different from operators and any regulation on OTT will be against the nature of the Internet. The opposing view argues that OTTs should have the same regulatory obligations as operators (such as taxes, licensing, emergency services and lawful interception) or that they should be paying operators to use their networks [7].

CCS'16, October 24 - 28, 2016, Vienna, Austria

ISBN 978-1-4503-4139-4/16/10. . . $15.00
DOI: http://dx.doi.org/10.1145/2976749.2978334

[1] Standardized by the ITU as E.164 phone numbers [4].

OTT from users' perspective.

While users enjoy the free communication services provided by OTT applications, they may also suffer from several security and privacy threats, as their personal data (such as contact lists, photos) is easily shared with these applications [29].

One issue that should concern all OTT users is the terms of service and end user agreements imposed by OTTs. A study shows that almost 70% of participants never pay attention to the terms of agreements and privacy policies while installing applications on their phones [15]. Moreover, it is impractical for users to read and understand the terms of service agreements of all the applications they are using [23]. As a result, OTT users may unknowingly accept terms of use that come with the end user agreements or default application settings.

Fraud detection in telephony networks.

Detecting the fraudsters in telephony networks is a challenging problem. Individual operators can deploy monitoring systems to trace calls within their network, but can not monitor calls once they are routed through another network, which is typical for international calls. The SS7 protocol [18], the core signaling protocol of the PSTN, does not provide a mechanism for tracing complete call route. This information can only be recovered when different operators collaborate. This is often difficult because of the variety and number of operators, fierce market competition and non disclosure agreements. Inevitably, operators lack the complete view of the network and fraudsters are difficult to identify.

1.1 Contributions

In this paper, we make the following contributions:

- We present the first comprehensive study of OTT bypass and position it in the current fraud ecosystem.
- We measure the importance and effects of OTT bypass fraud on a case study of a small European country[2]: technically, with experiments with more than 15,000 test calls over 8 months, and from the user perspective, with a large-scale user survey.
- We show various implementation flaws, as well as more fundamental problems that OTT bypass can cause in a network. We show that sometimes multiple fraud schemes collide, intensifying the degradation in service quality.
- Finally, we present evaluation criteria for multiple detection and measurement techniques and compare them.

1.2 Paper organization

This paper is organized as follows. In the next section we describe OTT in general and OTT bypass fraud. In Section 3, we present and discuss possible measurement techniques to evaluate the impact of the fraud. Then we present a case study of OTT bypass where we measure the impact of OTT bypass on a small European country (Section 4) and evaluate users' perception about it (Section 5). Section 6 presents the related work and we conclude in Section 7.

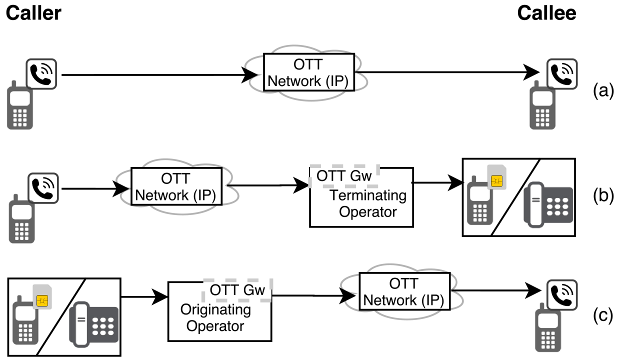


Figure 1: Types of OTT involved calls. a) Normal OTT usage, b) OTT-out, c) regular OTT-in.

2. OTT AND OTT BYPASS

2.1 OTT communication services

Compared to the traditional messaging (SMS/MMS) services and phone calls, OTT applications offer many additional features (e.g., group chat, video calling, photo, file or location sharing). Moreover, OTT services are usually free, whereas the traditional telephony services can be expensive.

On the other hand, due to the high competition in OTT market, it is challenging for OTT service providers to monetize their products: Users are usually not willing to pay for applications and they do not like advertisements. As a result, OTTs need to find other ways to make profit, such as the in-app purchases (e.g., for stickers and games [21]), and paid services that allow interconnection with the telephony network [17].

2.1.1 Telephony and OTT interconnections

To enable connectivity from the OTT service to the global telephony network, OTT providers partner with telecom operators[3] and use gateways between the OTT network and the PSTN. In this way, a call initiated from the OTT network can be terminated on the telephony network and vice versa. We will name these services as regular OTT *-in* and *-out* services.

The -out service allows to reach the telephony network from the OTT application, by terminating calls locally on callee's operator (Figure 1-(b)). This service is generally paid by the OTT user to cover the cost of the local call termination on the PSTN or mobile network.

The -in service (depicted in Figure 1-(c)) allows the OTT application to be reachable from any phone on the telephony network, by attributing a phone number to the OTT user. This phone number is often allocated for this kind of service, either by the telecom regulator, or indirectly through another service provider. All calls to this phone number are legitimately terminated over the application, by the OTT network. In this way, the caller can make a cheap local call and the OTT user can receive the call from anywhere in the world through the application. A common example of regular OTT-in service is provided by Skype. A user can purchase a *Skype number*, so that he can answer with Skype the calls initiated to this phone number.

[2] Because of legal concerns, we do not mention any operator names, the name of the bypassed country/operator or of the OTT application.

[3] They may also officially become operators themselves.

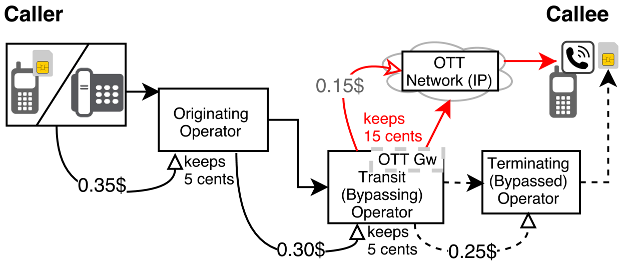


Figure 2: A normal call between 2 mobile phones in black and OTT bypass in red.

These OTT services are challenging the traditional telephony as they compete directly with telecom operator business. However, they legitimately use the telecom infrastructure and the attributed number ranges. They are also seen as a sign of healthy innovation and are generally accepted by users, even if some countries try to block or regulate them [28].

In this paper, we address a different kind of service which is called *OTT bypass*. We claim that OTT bypass is a fraud, because the bypassing parties earn non-legitimate benefits from it, while bringing revenue losses on operators and decreasing the service quality and stability for users. We will describe OTT bypass in detail in Section 2.4, but we first describe the money flow in international communications and the more common forms of interconnect bypass fraud.

2.2 Money flows in international calls

An international call originated from a mobile or fixed line, travels over multiple intermediate operators (transit operators) before reaching its destination country and operator. Each of these transit operators get a share from the call revenue for passing over the call, and the local operator in the destination country receives a *call termination fee* for terminating this international call on its network [12]. This regular international money flow is shown with black arrows in Figure 2.

International call termination fees may be artificially high in some countries due to monopolies, regulatory fees or taxes. Such revenue is often used to cover other costs such as network and infrastructure maintenance [1]. This is why call termination fees change from country to country, with small developing countries often having high termination fees. This makes them an attractive target for a type of fraud called *interconnect bypass*.

2.3 Interconnect bypass fraud

Interconnect bypass fraud aims to offer cheaper prices for international calls, by routing the calls fraudulently (*gray routes*). Examples of interconnect bypass include simbox fraud [41] and abuse of compromised Private Branch Exchanges (PBX) [27]. Simbox fraud often uses stolen SIM cards (or abuses SIM cards with cheap voice plans) inside a simbox (gateway between VoIP and GSM), which is used to inject international calls into the local telephony network, bypassing the international termination fee. PBX based bypass often abuses a compromised PBX for terminating international calls as national calls.

A fraudulent operator can attract international call traffic by advertising low call termination rates and then terminate this traffic over such *gray routes*. Despite constant fight against interconnect bypass, it is still an unsolved problem in telephony networks, with an estimated annual revenue loss of $5.97 Billion [6]. As we will show next, OTT bypass makes this problem even more challenging.

2.4 OTT bypass

OTT bypass requires agreements between telecom operators and OTT service providers to "bypass" calls. Such calls may originate from a landline or from a mobile number and are supposed to terminate on a mobile number. When a transit operator sees a call for a destination for which a bypass agreement exists, he will check with the OTT provider if the mobile number is registered and online on the OTT network. Many OTT smartphone applications use the mobile phone number as user ID, this greatly simplifies detection of phone calls which can be bypassed. The call will be redirected over the OTT service without the knowledge of the caller or acknowledgment of the callee[4] (or of their operators). OTT bypass is very profitable when the destination of the call has a high termination fee (often in developing countries). The price difference between the normal termination fee, and the negligible cost of OTT call received on a smartphone application becomes a source of revenue for the bypassing operator and the OTT service provider [16].

Unlike with other types of OTT-telephony interconnections, this does not benefit the end users, as the caller receives no cost reduction, the callee may pay to receive the call and, as we will show in this paper, the service quality is often seriously impaired.

Figure 2 shows a fictional example of a regular call from Country A to Country B, where the customer pays 35 cents per minute, operators carrying the call keep 5 cents each and the terminating operator collects 25 cents to terminate the call. In this way, the OTT provider proposes an agreement to the transit operator to terminate its calls for 15 cents/min. The transit operator keeps 15 cents per minute instead of 5 cents. Moreover, the OTT provider earns 15 cents per minute by taking over a call which is not intended to be sent over IP. On the other hand, the operator in Country B sees a reduction of its incoming international call traffic, and incurs financial losses due to the termination fees that are not perceived.

Throughout the paper, we call the operator who performs the bypass (the transit operator in Figure 2) the *bypassing operator*. In fact, the bypassing operator could be any of the transit operators on the route, or even the originating operator. All the subsequent operators are bypassed but we will call *the bypassed operator* the operator who is the main target of the bypass. In this paper we will further call bypassed incoming calls *incoming bypass*, i.e., the bypass from the view point of the terminating operator in Figure 2. Conversely, we will call *outgoing bypass* the bypass of outgoing calls, i.e., from the view point of originating operator in Figure 2.

To the best of our knowledge, the first trials to terminate traditional calls on OTT networks started in 2013 [17] and a patent was issued in 2014 describing this mechanism [10]. This patent also mentions that the OTT service provider may reject some bypass attempts. In this case, the bypassing operator can choose to route the call over another operator.

[4] As we will discuss later, the callee can opt-out from this default option.

This mechanism is very similar to the *crankback* functionality that is employed in some call routing protocols [39]. *Crankback* returns a call to the previous switch, so that it can choose another route (e.g., in case of congestion). The patent mentions transmitting the call twice, via the OTT provider and the traditional operator. The recipient's phone line and OTT application will ring simultaneously and the one that is not answered will be canceled. We show in Section 5 that this causes many problems for the users.

2.4.1 OTT bypass: A fraud or not?

It is often delicate to tell if some action is legal or not, especially when telecom operations are international with very diverse laws. We do not claim that OTT bypass is illegal (a lawsuit may be needed for this), but we claim that OTT bypass is fraudulent for the following reasons. Firstly, a call to a certain phone number has to be routed to the operator to which the phone number was allocated by International Telecommunication Union (ITU) or national regulators [4]. This is violated by OTT bypass, because the call is routed to the OTT provider instead. Moreover, most countries impose regulatory fees and taxes for incoming international calls. These are paid by the caller, but hijacked by the bypassing operator. Service level agreements between operators are also violated when an operator pays for a premium quality call route, but its calls are bypassed over the OTT network. Unlike many OTT services, OTT bypass has almost no benefits for the users. In practice, OTT bypass is similar (in its effects) to other types of interconnect bypass fraud, such as simbox bypass [41]. Finally, ITU recently created a working group to study OTT Bypass, where OTT bypass is clearly reported as a fraud [32].

2.5 Possible consequences of OTT bypass

Users may suffer from several problems when a call is bypassed over OTT. First, the call is going over the public internet, without any guarantees of call quality and with poor mobility management (moving away from a Wi-Fi area to mobile data network leads to an interruption). The callee will also be unable to use voicemail, call forwarding or call blocking services provided by his operator. The caller will pay the same fee for the bypassed call as he would pay for a normal call. However, the callee may be charged for data traffic while call reception is normally free, in most of the world, and may sometimes miss calls.

Effects of OTT bypass on bypassed operators can be more severe. All bypassed operators will suffer from a decrease in call volume. However, the terminating operator is likely to incur the highest revenue loss.

In the short term, OTT bypass is profitable to the bypassing operator. However, as the OTT provider expands its agreement coverage, it may be bypassed itself, as more traffic is terminated on OTT networks. Thus, OTT bypass and its effects should be considered globally, rather than individually by operators.

OTT bypass may also facilitate call hijacking: The registration verification is performed with a code sent over a regular text message. If an attacker is able to intercept such a message[5], he could register this account (phone number) on another phone. Using this technique, we were able to receive OTT bypassed calls on a phone that never had the corresponding SIM card. Finally, OTT bypassed calls may also evade lawful interception platforms.

3. DETECTION AND MEASUREMENT OF OTT BYPASS

Detecting the existence of OTT bypass and measuring its scale is important for bypassed operators to estimate losses, inform their customers and collect evidence for legal cases or in communication with regulators and bypassing operators. The main difficulty for a bypassed operator is to measure the traffic that is not flowing through his network anymore. We present possible techniques for detection and measurement of OTT bypass and we use the criteria presented in Table 1 to evaluate them (Table 2). While we focused on detection, most prevention techniques have to rely on detection first. In practice, multiple techniques can be combined to fight OTT bypass.

3.1 CDR volume analysis

Operators can observe the decrease in their incoming call traffic and generated revenue from the Call Detail Records (CDR). While this is an indicator, it does not provide a reliable measurement. Indeed, there may be other reasons for this decrease, such as regular OTT calls (other than OTT bypass) or changes of habits. Additionally, this technique can only measure effects of incoming bypass, but it is easy to implement and it does not interfere with the network and users' privacy (as long as CDRs are handled with care).

3.2 Tracking the OTT users' online status

OTT applications often automatically discover preexisting contacts on the network by using the address book (the so-called *address book matching* technique). This can be used to crawl registered phone numbers on an OTT network [14] and was also used for targetted attacks [29]. Similarly, contacts' online status displayed on the application can be monitored as well. Correlating this with the decrease of international calls for a large set of phone numbers could allow to estimate the amount of bypassed calls on the network.

We partially validated this approach by collecting online status of a test phone from the instrumented desktop application of the bypassing OTT provider. This allowed us to keep track of the online/offline status of the phone with 90% accuracy when compared to the actual online/offline status of the phone[6]. However, we did not perform such a large scale tracking of real users, due to the legal and privacy issues with this approach.

3.3 Test Calls

A more precise measurement is possible using test calls. There are many commercial Test Call Generation (TCG) platforms used for QoS testing and fraud detection[7]. TCG platforms provide call origination points worldwide, from various networks in various countries. Using a TCG platform, a bypassed operator can generate calls to its own network from various operators in the world. The bypassed operator needs to register some phone numbers to the OTT application and observe if the calls generated by the TCG

[5] E.g., through temporary access to the phone, a malicious application, or account hijacking [43].

[6] This experiment was conducted in a lab environment, with a rooted Android phone and a steady Wi-Fi network.

[7] e.g., Sigos, Revector, Roscom

Table 1: **OTT bypass measurement techniques evaluation criteria.**

Bypass direction	Detects either incoming or outgoing bypass
No collaboration requirements	Does not require collaboration of users, other operators or regulators
Easy deployment	Cheap and easy deployment, maintenance, no big changes to infrastructure
Scalable	Scalable to millions of users, applicable to different OTT vendors
Accurate	Does not detect legitimate traffic as bypassed traffic (no false positives)
Passive measurement	Measurements do not need intrusive setup, can be performed on past, logged data
Ethical and privacy preserving	Ethically feasible, respects users privacy
Complete	Detects all OTT bypass traffic (no false negatives or traffic which cannot be monitored)
Definitive	Not a cat-and-mouse game between operators and OTT providers
No privileged access required	Does not require access to some sensitive data or systems (e.g., CDR, network access)
Representative measurement	Gives a representative view of the bypass affecting the real call traffic
Technically easy	No potential obstacles foreseen in the deployment or implementation of the technique
Likely to succeed	Technique has been demonstrated work, or is very likely to work

Table 2: **Measurement techniques with their advantages and drawbacks (✓yes, ✗no, ~partially, ?unclear).**

	Incoming bypass	Outgoing bypass	No collaboration req.	Easy deployment	Scalable	Accurate	Passive measurement	Ethical/privacy	Complete	Definitive	No privilege req.	Representative measurmt.	Technically easy	Likely to succeed
Indirect evaluation (CDR analysis)	✓	✗	✓	✓	✓	✗	✓	~	✓	~	✗	~	~	~
Test calls for incoming and outgoing routes	✓	✓	✓	✗	✓	~	✓	✓	✓	~	✓	✗	✓	✓
Compare CDR with user status crawled on OTT network	✓	✗	✓	~	~	~	✗	✗	✗	~	✗	✓	✗	~
Pinpointing bypassing operators	✓	✓	✗	~	✓	✓	✗	✓	✓	✓	~	✗	✗	~
IP traffic analysis	✓	✗	✓	~	✓	✓	✓	~	✗	✗	✗	✓	✗	~
Audio fingerprinting (operator side)	✗	✓	✓	✗	~	?	✓	✗	✓	~	✗	✓	✗	~
Audio fingerprinting (caller side)	n/a	✓	✓	✓	✓	✓	?	✓	~	✓	~	✓	✗	~

platform terminate on the regular network or on the OTT application.

Unfortunately, these platforms are expensive ($1 to $10/test call), and often offer inflexible packaged services. Moreover, TCG platforms can only show the bypass on incoming routes. Checking for bypass on outgoing routes would require several phones deployed worldwide and with the OTT service installed (or abusing registration mechanism as mentioned previously). As far as we know, there are no such systems currently deployed.

Test calls shows bypass on tested routes but do not provide the bypass rate on the real traffic. The knowledge of the volume of calls on each particular route (before the bypass) and the market share of the OTT application is needed to estimate the actual bypass volume. However, routes can change quickly and it might be difficult to compute a good estimation of the actual amount of calls on each route.

3.4 Pinpointing bypassing operators

A major problem with OTT bypass is the opacity of the call routing. Because of this, discovering the bypassing operator is difficult. Some test call generation platforms provide information about the outbound route taken by a call. If a test call can be performed from the next hop indicated by the TCG platform, then this is one step closer to the bypassing operator. Iterating the tests in this fashion may allow to find who is performing the OTT bypass. However, this approach has multiple limitations, some of which we explain on a case study in the next section.

3.5 Network traffic analysis

As the OTT traffic is transmitted over the IP network, the operator may attempt to detect it in the data traffic [13, 19, 25, 33]. The main issue with this approach is that it will only allow to evaluate the OTT traffic from users who use OTT over the mobile data network, but not over other data networks from other operators (e.g., Wi-Fi/ADSL).

3.6 Audio fingerprinting

Like for simbox fraud [41], the OTT bypass may incur some distortion or particular fingerprints on the audio channel which may be used for detection. The caller or his operator could use audio fingerprinting to detect OTT bypass on outgoing calls. However, it seems difficult (in terms of resources) for an operator to fingerprint all audio communications. We could imagine to perform this detection from an application on caller's smartphone, but the call audio in smartphones is handled by the baseband processor and usually not available to the applications. Moreover, the incentives for the caller and originating operator to detect OTT bypass are not clear. In addition to this, the callee does not need detection, as he can see how he receives the call. Finally, the callee's operator can not fingerprint the calls because he can not access the audio stream of the bypassed calls.

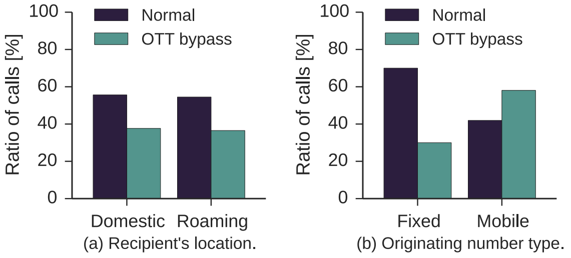
4. CASE STUDY: OTT BYPASS IN A SMALL EUROPEAN COUNTRY

In this section, we present a case study of OTT bypass performed on a mobile operator in a small European country. We mainly focus on test calls in our analysis, as the other techniques either have drawbacks (e.g., ethically questionable, unpredictable results) or would require a complete study on their own.

We next present results from two different test call campaigns in which 15,872 test calls were performed over a period of 8 months (summarized in Table 3). The first campaign was performed with a generic commercial TCG platform, with a very broad network coverage. In the second campaign, we performed more fine grained analysis using a

Table 3: Test calls performed during 8 months of experiments.

Origin	Number of calls	Duration	Date
Worldwide	1016	7 days	November '15
UK	134	3 days	March '16
Germany	260; 2876	4; 68 days	March; April-June '16
Netherlands	1220	55 days	May-June '16
Italy	3201	68 days	April-June '16
Switzerland	3635	67 days	April-June '16
Spain	1392	37 days	May-June '16
Austria	49; 2006	3; 37 days	April; May-June '16
Turkey	83	3 days	April '16
Total	15,872	352 test days	8 months



(a) Recipient's location.

(b) Originating number type.

Figure 3: Bypass rate depending on callee's roaming status and the type of originating call.

smaller and dedicated test call platform that we built for this purpose.

4.1 Global test with TCG platform

The TCG platform handles the generation of calls from various landline and mobile numbers that belong to different operators in different countries. For each call, the platform provides a call log including the originating country and network, call start time and call end time. At the receiver end, we use 4 different SIM cards that belong to the bypassed operator and that are registered to the OTT application. We collect the type of call termination from the recipient phones. We do not answer the calls, but only let them ring.

4.1.1 Measuring the prevalence of OTT bypass

1016 test calls were performed with the TCG platform, originating from 148 different networks (operators) in 50 different countries. OTT bypass occurred on calls originating from 90% of these countries and from 62% of the networks. In total, 40% of the test calls were bypassed. This shows that OTT bypass towards this destination is very frequent.

During those tests, the SIM cards were first in the home network (3 days) and then roaming in another country (4 days). The OTT bypass rates seem to stay the same whether the user is roaming or not, as shown in Figure 3-(a). With 95% confidence [35], bypass rates for domestic and roaming phones are 37% ±4.14% and 36% ±4.26% respectively. We also make a chi-square test to our hypothesis that the OTT bypass rate is independent of phone's roaming status. For the significance level of 0.05, p-value of the test is 0.713, which means that these variables are independent. This is consistent with the fact that the OTT bypass generally occurs before the call reaches the home operator and that a call to a roaming phone generally goes through the home operator first.

In Figure 3-(b), we analyze the effect of originating number type[8] on the bypass rate. With 95% confidence, landline numbers were bypassed with a ratio of 17% ±4.57% and mobile numbers were bypassed with a ratio of 25% ±4.12% [9]. The bypassing operator may be processing all the calls in the same way, regardless of the originating number type. We note that, the reception of calls from a landline on the OTT application may be surprising for a callee who is not aware of how OTT bypass works.

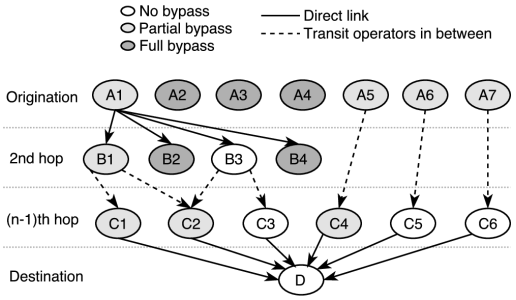


Figure 4: Partial map of operators involved in test calls originating from UK.

4.1.2 Identifying bypassing operators

For some of the calls (usually the calls that are originated from landline numbers), the TCG platform also provides the name of the outbound operator. For a non-bypassed call, the mobile operator sees the call arriving from the inbound operator, which we obtained from SS7 logs.

Figure 4 shows the result of combining those logs to build a partial map of routes for the calls originating from 7 different operators in UK. We see that all calls initiated from operators A2, A3 and A4 are bypassed. Those operators may be using a fraudulent route, or they may be the bypassing operators themselves. For operator A1, we are able to see the first level of transit operators (B1, B2, B3, B4). A1 suffers from bypass, every time it selects the operators B2 or B4 for routing the calls. Moreover, operator B1 should have at least one bypassing operator among its immediate or subsequent partners. This is also valid for operators A5, A6 and A7. With this information, we could already start to identify problematic routes and potential bypassing operators.

Pinpointing the exact bypassing operator on a route would be possible by iterating over the route (for example make test calls from B1, on all its possible routes to artificially "trace" a call) to identify the next hops and which of them perform a bypass, until the home operator is reached. This approach would require that (1) the calls will follow the same route when bypassed or not (until the bypass), (2) that a call will be routed similarly when traversing and when originated by a network (3) routes are stable over time and (4) we obtain the next hop for each operator on the route.

However, assumptions (1) and (3) do not always hold because route selection can be very dynamic, depending on the contractual agreements and routing algorithms. We also found cases where operators show different bypass behavior when they are in transit or originating positions. For ex-

[8] Determined using a numbering plan database [2].

[9] Using the test calls for which we have the originating number (74% of the test calls).

ample, all calls originated from operators C1 and C2 were bypassed even though they have transit agreements with the home operator. Finally, assumption (4) may not hold as the TCG platform may not always provide the next hop information.

Due to these limitations and the high cost of the TCG platform, we were not able to perform such iterative test calls to reveal a larger map of operators.

4.2 Fine grained experiment with our custom test platform

In order to run long-term, customized tests, we used a small test call generation platform that we built from scratch. Our platform is built on Android phones that we control remotely via SSH on a Wi-Fi connection. We generate calls from one Android phone (caller) to another (callee). For each test call, we collect information from both phones. For normally terminated calls, we also obtain the Call Data Records (CDR) from the home operator (Figure 5). All events are timestamped and phones are synchronized with NTP. With this setup, measurements have an accuracy of 20 milliseconds or better. Again, we do not answer any calls, but let them ring for one minute.

To generate test calls, we placed one phone per country, in 8 European countries. Even though we could test only one originating operator per country, all of them were major operators, with a total of more than 100 million customers. For each generated test call, we collect the network name, call start time, ringing time and call end time from the caller. Because the network conditions may change during the day, we initiate the test calls at every hour of the day, from each of the operators.

On the receiving side, we use 3 smartphones each with a SIM card from the bypassed operator. Two of them are registered on the OTT network and one of them was never registered. One of the registered SIM cards is used with changing configurations such as connectivity on/off and OTT bypass option[10] enabled/disabled. We collect the incoming call logs from the relevant database files in Android and the OTT application. Using these logs, we obtain the incoming call time, call termination type and the received caller ID. Moreover, the recipient phones are roaming in another European country (visited country), outside of their home country, as depicted in Figure 5.

4.2.1 Bypass rates and colliding fraud schemes

During our experiments, we noticed that multiple fraud schemes sometimes collide. In a few cases, we detected other types of interconnect bypass (via simbox and PBX) in addition to OTT bypass (Figure 5) and a possible case of *false answer supervision fraud* which we will explain later.

We detect the simbox and PBX bypass frauds by comparing the real caller ID and the received caller ID. An incorrect caller ID often means that the call went over an illegitimate gateway, which modified the caller ID.

If the Caller ID corresponds to a mobile phone number range, we assume the call was bypassed with a simbox. On the other hand, if the number belongs to a fixed range we assume this is a PBX bypass (we also check how the number was allocated). In fact, a PBX may allow to spoof a caller ID, but this is not possible with simboxes, as they essentially use an IP-GSM gateway. Thus, caller ID inconsistencies remains a good indicator of interconnect bypass. In particular, we expect false negatives (forged caller ID) but no false positives.

Table 4: Simbox and OTT bypass combined.

	OTT Not Registered	OTT Registered, Online
Normal calls	38%	22%
Simbox bypass	62%	17%
OTT bypass	-	35%
Simbox + OTT bypass	-	26%

We observed up to 83% OTT bypass rate from 6 out of 8 countries (Figure 6-(b)). We now describe interesting observations on those test calls.

Simbox and OTT bypass collision.

The test calls performed from UK in March had a ratio of 61% of OTT bypass. Some of the calls were also bypassed over a simbox, that uses SIM cards from a mobile operator from another country. Table 4 shows the bypass rates for two different recipient phone numbers, one is registered to the OTT application and the other is not. The overall simbox bypass rate is 43% if the number is registered on the OTT network and 62% otherwise. We have collected 34 unique simbox numbers, belonging to the same operator.

We observe that 26% of the calls to the OTT registered phone number were bypassed first over the simbox (② in Fig. 5) and then over the OTT network (③ in Fig. 5). In other words, the operator on which the simbox bypass occurred routed the call over a route which is subject to OTT bypass. However, not all the OTT bypassed calls had simbox caller IDs. Thus, there should be another operator performing OTT bypass on a different route, or before the simbox bypass (such as ① in Fig. 5). We also confirm this when we make calls while the phone is offline (has no internet connectivity). For example, we make a call to an offline phone but the phone does not receive the call (does not ring). Then we turn on the connectivity and get 2 different missed call notifications on the OTT application: one with a correct caller ID, and one with a simbox caller ID. In other words, each time there is an attempt to send the call over OTT network, the OTT application receives a missed call notification.

PBX bypass on roaming part of the call.

We observed another interconnect bypass fraud, through possibly compromised cloud IP-PBXs[11]. In this case, a test call arrives with a caller ID belonging to a fixed phone number, with a geographic area code from the visited country. However, we never observe an OTT bypassed call with a PBX caller ID. Also, the call data records from the bypassed operator show the correct caller ID. This PBX bypass therefore occurred between the bypassed operator and the visited operator (④ in Fig. 5). As a result, a call bypassed over the OTT network has a correct caller ID, but a call terminated normally may have an incorrect caller ID. Figure 6 summarizes the bypass rates for two different recipient phone numbers, one is not registered on the OTT application (only experiences PBX bypass) and the other is registered and on-

[10] The application setting that allows OTT bypass

[11] The phone numbers were allocated by the regulator to this cloud PBX service provider, this interpretation was also confirmed by an operator who was aware of this bypass case.

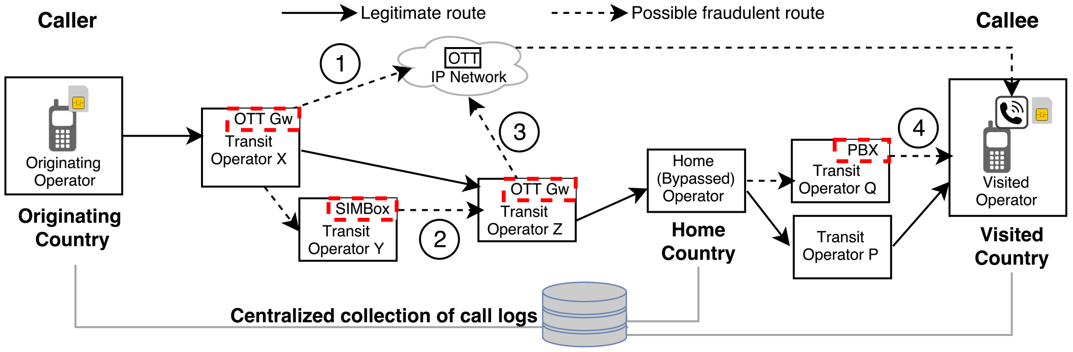
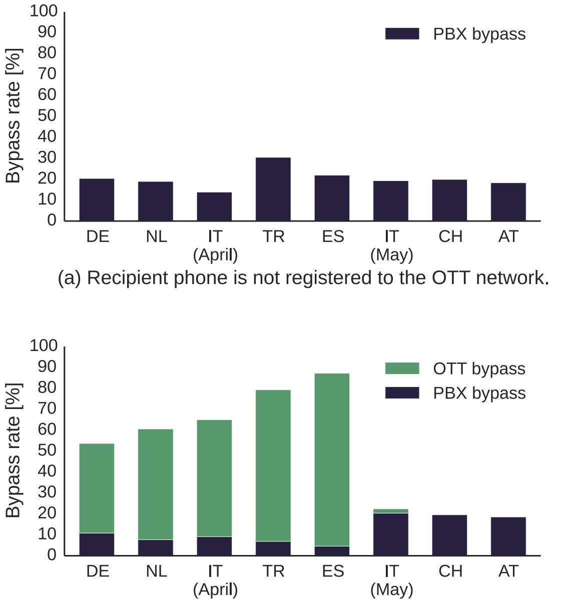


Figure 5: Experimental setup and summary of fraudulent routes.



(a) Recipient phone is not registered to the OTT network.

(b) Recipient phone is registered to the OTT network, online.

Figure 6: OTT and PBX bypass rates depending on the phone status.

line on the OTT network (experiences both PBX and OTT bypass). We can see that, among the countries that experience OTT bypass, PBX bypass rates are relatively lower for OTT registered phones because most of the call volume is terminated over the OTT network.

False Answer Supervision (FAS) fraud.
Among the 8 countries we analyze, Spain has the highest percentage of fraudulent calls: 88% of calls were subject to either OTT or PBX bypass. From Spain, we detect many other problems: 17% of normal call terminations have an empty caller ID and 30% of the calls did not reach their destination (counted as failed calls). Moreover, we were charged for 23% of the calls in the first 10 days of the experiment, even though we do not answer any of the test calls. In addition, half of the calls that were illegitimately billed, were actually failed calls. These issues probably stem from a fraudulent gateway on the call route, which employs False Answer Supervision (FAS) fraud. FAS is a common fraud [5], where a transit operator starts billing the call while the call is ringing, but not yet answered. The fraudulent transit operator may also divert the call to a fake ringing tone or network message and bill the call as if it was answered, without routing it to the legitimate destination [3].

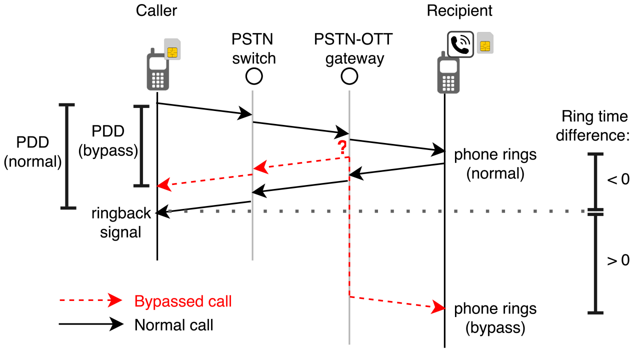


Figure 7: Post Dial Delay (PDD) in a normal phone call and in a OTT bypassed phone call.

4.2.2 PDD analysis and ringing anomalies

The Post Dial Delay (PDD) is the interval of time between the press of the call button (or the last digit of the phone number) and the ringing tone, if the call establishment is successful, or any other network message indicating the call outcome [31, 38]. The PDD covers the connection establishment process in which multiple switches and gateways are involved in setting up an international call. It is one of the main QoS metric in telecommunication networks [42] because it affects caller's perception of the state of the call setup and, e.g., her decision to abandon the call [37, 38]. The International Telecommunication Union (ITU) specifies a recommended mean PDD value of 8 seconds for international PSTN calls and 16.5 seconds for international mobile calls [30, 31].

VoIP to PSTN gateways generally increase the complexity of call setup process and they often introduce additional performance problems [16, 22]. Thus, we expected the bypassed calls to have higher PDDs (i.e., *PDD (bypass)* in Figure 7) would be larger than *PDD (normal)*).

Surprisingly, we found that values for OTT bypassed calls are very similar to those for normal calls (Figure 8). Moreover, for 2 countries, Germany and Turkey, the mean PDD

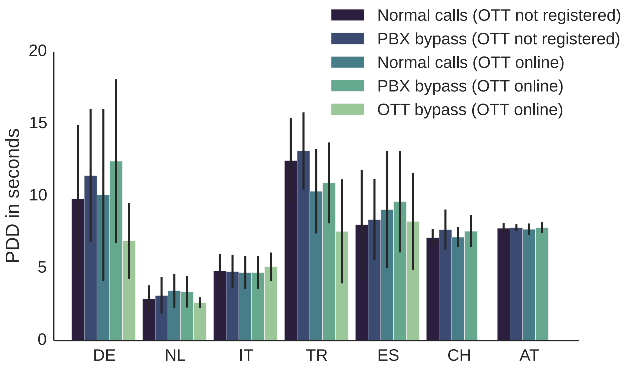


Figure 8: Mean PDD and standard deviation, for each country in function of the bypass type (no OTT bypass for 2 countries).

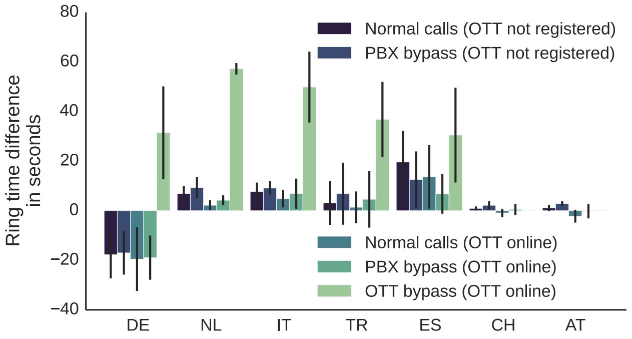


Figure 9: Mean ring time difference and standard deviation, for each country in function of the bypass type (no OTT bypass for 2 countries).

values for OTT bypassed calls are even smaller than for normal calls. We therefore also measured the time difference between the recipient phone ringing and the caller hearing the ringing tone. We call this the *ring time difference*. As we demonstrate in Figure 7, if the callee's phone starts ringing first, and the caller hears the ringing tone later, ring time difference becomes a negative value. On the other hand, if caller hears the ringing tone first and the callee's phone starts ringing later, this value will be positive. Ideally, the ring time difference should be close to 0, so that the caller and callee are be notified simultaneously. While a small ring time difference is normal, we found that it is much higher for OTT bypassed calls than normal calls (Figure 9). This seems to indicate that the OTT provider sends a false ringing tone to the caller, before the recipient's phone actually starts ringing. In other words, during the 30-40 seconds of ring time difference interval, the caller will think that the recipient's phone is ringing, but the recipient will not be notified about this call. As a result, caller may drop the call before the callee is aware of the call or has time to answer. This practice should not be confused with false answer supervision fraud, because here even if the caller hears an early ringing tone, the calls do not start to be charged.

4.2.3 Implementation related problems

OTT bypass requires a good synchronization between the bypassing operator and the OTT provider. Implementation or configuration mistakes may lead to unexpected problems.

The OTT provider needs to check if the user is online and has a proper Internet connection before bypassing a call. This can be done in several ways such as using periodic data probes or using historic data from past calls and locations. Failing to do this accurately can lead to two problems. First, when a user receives a call but recently went offline on the IP network, the OTT provider may still try to bypass the call. Because the user is offline, he will miss the call, even if his phone was in fact able to receive it as a regular call. When he is back online, he will receive a missed call notification from the OTT network. Secondly, when the phone is currently offline and unreachable from the cellular network, e.g., in airplane mode, the calls may still be bypassed. I.e., the caller may hear a ringing tone, instead of getting a network message (or voicemail) indicating that the callee is unreachable.

It is possible that the parallel calling feature (described in Section 2.4) was introduced to hide such problems. With this feature, the bypassing operator notifies the OTT provider and another transit operator at the same time. Thus, even if the OTT provider is not able to terminate the call, the transit operator will try another route to terminate it. As a consequence of this, the user may get a missed call notification on the OTT application even when a call was received normally.

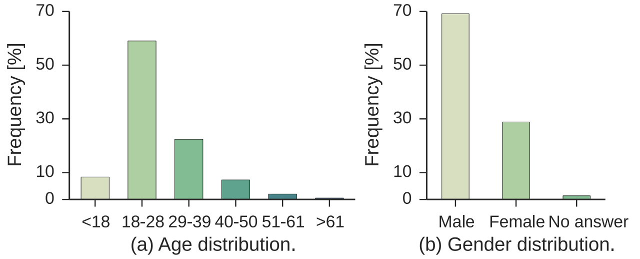
We highlight these problems by conducting a dedicated experiment where we turn off the Internet connectivity off and on and then we switch the phone off and on, waiting for 5 minutes between each step. During the 5 minutes period, we initiated 5 calls to this phone, one call per minute. We do this several times (60 calls in total). We found that 60% of the calls were terminated normally, but left a missed call notification on the OTT application while the Internet connectivity was off. Moreover, the caller heard a ringing tone in 20% of the calls even though the recipient phone was turned off. These problems are also mentioned by the users (Section 5.1).

4.2.4 Discussion

Our experiments show that telephony networks are subject to a high amount of fraud, which deteriorates call quality. It seems that OTT bypass often collides with other forms of bypass. This may be due to a "race to the bottom" on the price of call minutes. For example, when an operator receives an artificially low price for a destination due to the presence of OTT bypass, then it might make good offers to its customers for that destination. These low offers may in turn be abused by simbox fraudsters.

Even though the OTT provider seems to conceal some of the effects of OTT bypass, those effects further degrade the quality of call establishment.

Note that, we did not measure audio quality in our test calls, because OTT bypass does not necessarily deteriorate it. Instead, we have focused on other aspects of QoS, which are fundamentally harder to solve in an OTT bypass scheme. Moreover, as we mentioned in Section 3.6, call audio is not easily accessible on smartphones and it would be costly to answer the test calls.



(a) Age distribution.

(b) Gender distribution.

Figure 10: Age and gender distribution for participants.

5. CASE STUDY: USER STUDY

In this section we present a user survey conducted on 8,243 customers of the bypassed operator which we studied in the previous section.

Understanding users' perception and experience on OTT applications can provide insights on how to address the issues with OTT bypass. We therefore performed a large-scale survey where we first aim to measure the *perceived QoS* [26] (customers' experience of using the OTT services). Then we measure the *assessed QoS* (i.e., customer's decision on whether to continue using the service). Thus, in this survey we measure:

- OTT usage frequency, experience and habits (perceived QoS),
- the awareness about OTT bypass option,
- the tendency to opt-out from OTT bypass option, after informing users about its effects (assessed QoS).

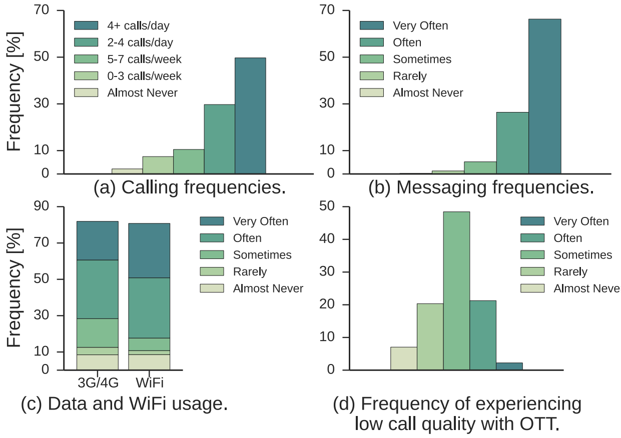
5.1 Organization of the survey

The survey consists of 12 questions. We prepared the survey to be short, easy to answer, and to be as neutral as possible. It was mainly advertised for users of the bypassing OTT provider, via the mobile operator's social media pages and call center. As an incentive, a bundle of 2 GB of free mobile data for 3 months was offered to 10 randomly selected participants. This attracted many responses, but also helped to ensure that only real customers answered the survey as the phone number had to be provided to obtain the prize. The survey received 8,739 answers, out of which 7,617 were left after removing the duplicates[12] and answers from people who claimed they do not use the bypassing OTT application. The questions were written in English and then translated to the local language. A 5-level Likert scale [36] is used in most of the questions. The rest of the questions are either yes/no or open ended questions.

5.2 Results on general OTT usage

The first five questions of the survey address the general OTT and smartphone usage. Figure 10 shows that the majority of the participants are young adults and 70% of participants are male.

Figure 11-(a) and (b) show that OTT applications are very popular for both calling and messaging. This can also indicate that a significant percentage of voice and messaging traffic is carried by OTTs. Moreover, 72% of OTT users are using it for international or both international and domestic calls.



(a) Calling frequencies.

(b) Messaging frequencies.

(c) Data and WiFi usage.

(d) Frequency of experiencing low call quality with OTT.

Figure 11: Statistics on the usage of OTT applications.

Another point we analyze is the frequency of use of Wi-Fi and mobile data networks. Figure 11-(d) shows that both Wi-Fi and data use is very common, yet the Wi-Fi usage is slightly more frequent. This is an important observation, because when the Wi-Fi network is used, the operator will not see the OTT bypass IP traffic at all. Moreover, the fact that OTT users stay online most of the time increase their chances to be a victim of OTT bypass.

In figure 11-(d), we can see that people frequently experience call quality problems (such as distorted audio, incorrect caller ID and call failures) with OTT applications. 70% of participants experience problems, 'Sometimes' or more often.

5.3 Results on the usage of the OTT service

After analyzing overall OTT usage, we ask 5 questions only related to the bypassing OTT provider.

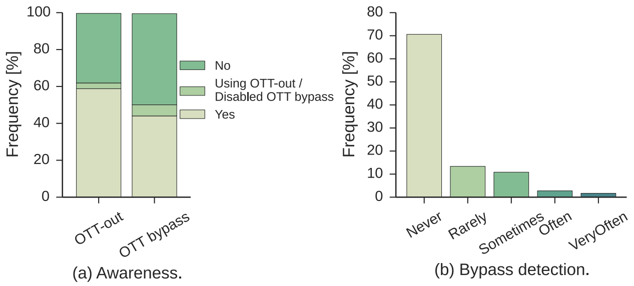
We first remark that this OTT provider has a *OTT-out* service, which is a regular OTT service as we described in Figure1-(b). The *OTT-out* feature is advertised a lot, whereas the OTT bypass option is only shown in the application's settings and in the terms of service, e.g., even the OTT provider's web page does not mention it. Moreover, OTT bypass option is enabled by default and users can opt-out from it inside the application settings.

5.3.1 Awareness about OTT bypass option

We compare the user awareness about the prominent OTT-out feature and the buried but active by default OTT bypass option. Figure 12-(a) shows that awareness of the OTT bypass option (50%) is lower than the awareness of the OTT-out feature (62%). However, number of people who have deactivated OTT bypass is higher than the number of people who are using OTT-out: Among the people who are aware of OTT-out, 5% are actually using it, but among the people who are aware of OTT bypass, 12% have deactivated it. Apparently, OTT-out feature is not very popular among the participants.

We consider OTT-out users as more advanced users, who may check the settings and who can better understand the

[12] Only the first answer for each customer (phone number) was kept.



(a) Awareness.

(b) Bypass detection.

Figure 12: Awareness on different application options and bypass detection rates.

meaning and consequences of the OTT bypass option. Among them, 73% were aware of the OTT bypass option, and 20% have deactivated it. Thus, it is likely that knowing and understanding more about the OTT bypass option increases the deactivation rate.

5.3.2 *Bypass detection*

Another goal of this survey is to understand participants' experience with OTT bypass. Figure 12-(b) shows that, 30% of people think that they have received at least one bypassed call. Among the people who frequently receive bypassed calls (often or very often), 28% were previously not aware of the disable option, 64% were aware and 8% have already disabled. Quite a high proportion of users was aware of the OTT bypass option, but did not opt out. There are two possible reasons for not disabling the OTT bypass option. First, it is possible that people do not actually understand the effects of this option. Second, people may not be experiencing any problems with it, so they leave the option as default [34]. Then, we ask, in an open ended question, if participants detect any calling anomalies with the bypassing OTT application. 53% of people answer *No* to this question while 0.6% answer *Yes* and 1% enter a long answer with additional comments. Some of these comments are not related to our discussion, such as problems with video calls or registration issues. However, some of the answers highlight important issues and confirm the problems we found in Section 4:

- The application does not ring during an incoming call, but shows notification afterwards
- Users appear online on the application, even when they do not have Internet connectivity
- Caller hears ringing tone, even when recipient is not online
- Multiple call notifications are received for a single call
- Poor quality or interrupted calls (delays, noise)
- Receiving an international call from a landline on the OTT application

5.3.3 *Opt-out analysis*

Finally, after we inform the participants about the effects of OTT bypass option, 45% of participants stated that they consider opting out on this option. Among the people who frequently detect bypassed calls and who were previously aware of the OTT bypass option, 39% consider opting out. This shows that, incoming OTT bypass can be reduced by increasing customers' awareness about the effects of the bypass.

5.4 Discussion

This survey demonstrates the dependence of users on OTT applications, despite the quality problems they experience. Most people are likely to use OTT applications as a cheaper alternative to traditional communications. However, users rarely pay attention to the details of the terms of use. The fact that OTT bypass option was known by 50% of people, but it was disabled by only 12% leads to think that this option was not carefully reviewed by most of the people or is not well understood. Therefore, operators can work on increasing customers' awareness on OTT bypass fraud and informing application users about the deactivation option.

6. RELATED WORK

Various solutions are proposed to detect and prevent interconnect bypass fraud in the literature.

In [20], a supervised learning algorithm is used to detect simbox fraud. The dataset is gathered from a mobile operator and it includes CDRs from both legitimate subscribers and a fraudulent simbox. The proposed classifier has 98.7% accuracy in identifying the SIM cards that are used in the simbox device. A similar study is conducted in [40], with a much larger dataset and different set of features used for classification. This analysis shows that simboxes are usually static, they connect to a few base stations and they initiate a significant number of calls. These solutions are not applicable to OTT bypass, because (i) there is no single hardware that performs bypass, (ii) detection of OTT application itself is useless, (iii) the bypassed calls may never go over the terminating party's operator and no CDRs will be available for bypassed calls. Audio fingerprinting can be used to determine call provenance [9]. A more recent study analyzes the degradation in call audio caused by the VoIP-GSM gateways, to detect simboxes [41]. This technique may be applied to detect outgoing OTT bypass calls on caller's operator or phone, as discussed in Section 3.

Identifying OTT traffic in the network is challenging, as the applications are usually obfuscated, communicating over encrypted channels and use proprietary protocols. Various studies try to detect and classify Skype traffic flows using pattern detection, machine learning and protocol identification techniques [13, 25, 33]. Similar approaches can identify other OTT applications, but only provide a partial solution to the OTT bypass problem.

6.1 Commercial solutions

While OTT bypass is a recent form of telecom fraud, there are already commercial offers for detection and blocking of OTT bypass[13]. Public documents do not clearly distinguish between detection and prevention, more information is only available under NDA. Those offers seem to focus on bypass detection using test calls, and then, possibly, use DPI (Deep Packet Inspection) probes to block OTT IP traffic. It is unclear if the DPI probes are able to block the OTT bypass IP traffic only or if all OTT traffic is blocked (which could raise serious network neutrality problems). OTT bypass traffic

[13] http://www.revector.com/, http://www.sigos.com/, http://purgefraud.com, http://www.araxxe.com

could be impossible to distinguish from plain OTT traffic, but in practice some differences may be exploited.

7. CONCLUSION

OTT bypass aims at terminating traditional calls on OTT network, while being seamless to both the caller and the callee. In this study, we show that OTT bypass is far from being seamless: communication quality is affected in various ways and users experience problems with it. While we focused on detection and measurement, more research is needed for the prevention of OTT bypass fraud, without disrupting regular OTT communications and violating network neutrality.

Fighting OTT bypass fraud requires a cooperative effort between the different parties that are affected. We have shown that informing users about the consequences of OTT bypass may be the first step to reducing it. Thus, increasing awareness and collaboration between operators, regulators, and users can help to work towards a definitive solution.

8. ACKNOWLEDGMENTS

The research was partially funded by the Principality of Monaco. We also thank anonymous reviewers, the people who hosted test phones and operators we worked with, for their invaluable comments and support in conducting the experiments.

9. REFERENCES

[1] Alternative calling procedures: Background and trends. ITU, World Radiocommunication Conference, 2012.

[2] BSMilano, Worldwide National Numbering Plans Collection. http://bsmilano.it/.

[3] Details about fas (false answer supervision). Nexmo Knowledge base, 2016.

[4] The international public telecommunications numbering plan. ITU-T Recommendation E.164, 1997.

[5] Subex wholesale fraud management survey 2013. Subex Limited, whitepaper, 2013.

[6] Communications Fraud Control Association (cfca), 2015 global fraud loss surveys, 2015.

[7] Smart regulation for OTT growth. Asia Internet Coalition, whitepaper, October 2015.

[8] New threat to mobile network operator revenues. Revector Company Blog, February 2016. http://www.revector.com/index.php/new-threat-ott/.

[9] V. A. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. T. Hunter, and P. Traynor. Pindr0p: Using single-ended audio features to determine call provenance. CCS '10, pages 109–120, New York, NY, USA, 2010. ACM.

[10] M. Barth. M. barth, call termination on ott network, patent wo 2014087269 a4. Patent WO 2014087269 A4, 2014. Patent WO 2014087269 A4.

[11] M. D. Bhawan and J. L. N. Marg. Consultation paper on regulatory framework for over-the-top (OTT) services. Telecom Regulatory Authority of India, March 2015.

[12] C. Bignell. The different frauds: Interconnect bypass. Revector, Fraud for thought blog, August 2012.

[13] D. Bonfiglio, M. Mellia, M. Meo, D. Rossi, and P. Tofanelli. Revealing skype traffic: When randomness plays with you. *SIGCOMM*, 2007.

[14] Y. Cheng, L. Ying, S. Jiao, P. Su, and D. Feng. Bind your phone number with caution: Automated user profiling through address book matching on smartphone. AsiaCCS'13, 2013.

[15] E. Chin, A. P. Felt, V. Sekar, and D. Wagner. Measuring user confidence in smartphone security and privacy. SOUPS '12, 2012.

[16] E. Coll. *Telecom 101: Third Edition*. Teracom Training Institute, 2008.

[17] J. Crook. Viber is testing new revenue models, value-add features by integrating with traditional telephony. TechCrunch, July 2013.

[18] L. Dryburgh and J. Hewett. *Signaling System No. 7 (SS7/C7): protocol, architecture, and services*. Cisco press, 2005.

[19] S. Ehlert and S. Petgang. Analysis and signature of skype voip session traffic. 2006.

[20] A. Elmi, S. Ibrahim, and R. Sallehuddin. Detecting sim box fraud using neural network. In K. J. Kim and K.-Y. Chung, editors, *IT Convergence and Security 2012*.

[21] eMarketer. Digital content and advertising key revenue generators for messaging apps. emarketer, November 2015.

[22] T. Eyers and H. Schulzrinne. Predicting internet telephony call setup delay. In *First IP Telephony Workshop*, 2000.

[23] C. Fiesler and A. Bruckman. Copyright terms in online creative communities. In *CHI*, 2014.

[24] Fisher Investments. *Fisher Investments on Telecom*. Wiley, 2011.

[25] E. P. Freire, A. Ziviani, and R. M. Salles. Detecting skype flows in web traffic. In *NOMS 2008*, April 2008.

[26] J. Gozdecki, A. Jajszczyk, and R. Stankiewicz. Quality of service terminology in IP networks. *IEEE Communications Magazine*, 2003.

[27] M. Gruber, C. Schanes, F. Fankhauser, and T. Grechenig. Voice calls for free: How the black market establishes free phone calls - trapped and uncovered by a voip honeynet. In *IEEE Privacy, Security and Trust (PST) 2013*.

[28] S. Guerraoui. Morocco banned skype, viber, whatsapp and facebook messenger. it didn't go down well. middleeasteye.net, 9/3/2016.

[29] S. Gupta, P. Gupta, M. Ahamad, and P. Kumaraguru. Abusing phone numbers and cross-application features for crafting targeted attacks. *CoRR*, abs/1512.07330, 2015.

[30] Network grade of service parameters and target values for circuit switched public land mobile services, ITU, rec-e.771, 1996.

[31] Network grade of service parameters and target values for circuit-switched services in the evolving ISDN, ITU, rec-e.721, 1999.

[32] ITU Study Group 3, Question 9/3. Ott bypass. International Telecommunication Union: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10892#TOP, march 2016. Editors: Rim Belhassine-Cherif and Chafik Jallouli.

[33] M. Korczynski and A. Duda. Classifying service flows in the encrypted skype traffic. In *2012 IEEE ICC*, pages 1064–1068, June 2012.

[34] Y.-L. Lai and K.-L. Hui. Internet opt-in and opt-out: Investigating the roles of frames, defaults and privacy concerns. In *ACM SIGMIS CPR*, 2006.

[35] J.-Y. Le Boudec. *Performance evaluation of computer and communication systems*. Computer and communication sciences. EPFL Press London, Lausanne, 2010.

[36] R. Likert. A technique for the measurement of attitudes. *Archives of Psychology*, 142:1–55, 1932.

[37] S. J. Lupker, G. J. Fleet, and B. R. Shelton. Callers' perceptions of post-dialling delays: the effects of a new signalling technology. *Behaviour & Information Technology*, 7(3):263–274, 1988.

[38] V. Matić, A. Lebl, D. Mitić, and M. Dukić. Estimation of post dialling delay in telephone networks. *Przeglad Elektrotechniczny*, R. 88, nr 5b:154–156, 2012.

[39] D. Medhi and K. Ramasamy. *Network routing - algorithms, protocols, and architectures*. Morgan Kaufmann, 2007.

[40] I. Murynets, M. Zabarankin, R. P. Jover, and A. Panagia. Analysis and detection of simbox fraud in mobility networks. In *INFOCOM*, 2014.

[41] B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor. Boxed out: Blocking cellular interconnect bypass fraud at the network edge. In *USENIX Security*, 2015.

[42] J. S. Richters and C. A. Dvorak. A framework for defining the quality of communications services. *Comm. Mag.*, 26(10):17–23, oct 1988.

[43] S. Schrittwieser, P. Fruhwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. R. Weippl. Guess who's texting you? evaluating the security of smartphone messaging applications. In *NDSS*, 2012.

[44] N. A. Wasmi. Telecoms regulator says viber is 'unlicensed' in the UAE, September 2014. The National UAE.