sandvine®

Intelligent Broadband Networks

2017 Global Internet Phenomena

SPOTLIGHT: OTT VOICE BYPASS FRAUD

sandvine
Intelligent Broadband Networks

Global Internet Phenomena Spotlight: OTT Voice Bypass Fraud

As the use of Voice over IP (VOIP) grows due to its wide adoption as part of Over-the-Top (OTT) applications, its integration with the many decades old SS7 interconnect agreements are a growing cause of concern for end subscribers, regulators and obviously communication service providers.

As this study shows, there is a growing number of occasions where PSTN voice calls are routed through VOIP connections, exposing these communications to a variety of security and privacy threats.

Measuring the extent of the exploitation of the security flaws in the voice network can help an operator make data-driven decisions about where to invest to secure it, how to report to the regulator, the risk to the security and privacy of their subscribers, and can help build a mitigation plan to reduce the OTT voice bypass fraud impacts.

Interconnect Bypass Fraud Background

Fraud is a growing challenge for communications service providers (CSPs) around the world.

While CSPs have dealt with many of the more traditional fraud cases shown in the chart below, there are growing concerns around the use of voice over IP (VoIP) as a means to defraud CSP interconnect agreements.

According to a recent survey by the Communications Fraud Control Association[1], Interconnect Bypass fraud is one of the largest causes of lost revenue costing communications service providers across the globe an estimated $6 billion dollars (United States Dollars) annually.

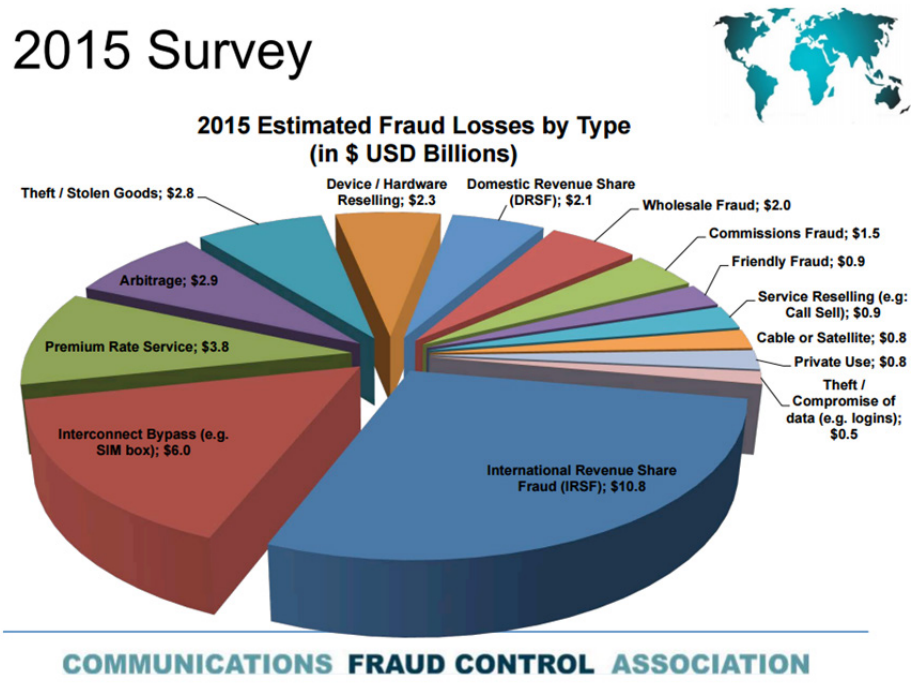

Figure 1 - 2015 Estimated Telecom Losses by Fraud Type

Interconnect Bypass fraud is lucrative because CSPs have agreements with each other where interconnection fees are paid for any inter-CSP call that is routed through or terminates within their network. For example, a call originating in the United States but destined for Brazil could travel through networks in Mexico and Colombia before reaching the end user. In this instance, a portion of the per-minute fee paid by the user would go to each of the networks through which the call is routed.

1. 2015 Global Fraud Loss Survey: http://cfca.org/fraudlosssurvey/2015.pdf

Until recently, the majority of Interconnect Bypass fraud was attributed to "SIMbox[2] fraud," which involved connecting SIMboxes into the SS7 interconnect to bypass traditional voice call routing via a VoIP connection. A SIMbox contains many SIM cards which allow a fraudulent actor to route calls through VoIP which dramatically reduces the fees paid to the terminating CSP.

OTT Voice Bypass Fraud

In recent years, however, the explosion of mobile VoIP applications has helped to introduce a new type of fraud: OTT Voice Bypass fraud. This new form of fraud is now on the rise, through exploitation of VoIP applications that offer the ability to hijack phone calls by fraudulent actors.

These applications typically include a feature known as "In Calling." If an OTT VoIP app offers an "In Calling" feature, it allows individuals to receive incoming calls from numbers that are not associated with the OTT VoIP app. As a result, fraudulent actors are able to use the "In Calling" feature to replicate the Interconnect Bypass fraud seen with SIMboxes, by using the OTT VoIP apps in place of SIM cards.

The exploitation of security flaws in the SS7 voice network by OTT VoIP apps present significant security and privacy risks for subscribers, and significant lost revenue risks for CSPs.

Figure 2 below shows the experience that many consumers expect when using an app that enables OTT VoIP Calls. In this instance, a subscriber knowingly initiates a VoIP call using an OTT VoIP app to another subscriber who also has the same app. In a call like this, a peer-to-peer protocol is typically used to establish a connection between both parties.

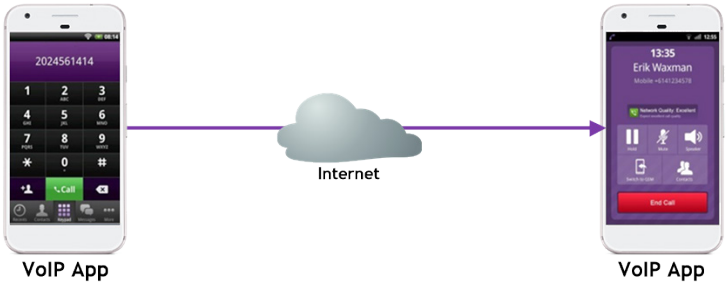

Figure 2 - OTT VoIP to OTT VoIP Call

Figure 3 below shows how the "In Calling" feature of some OTT VoIP apps are used to commit Interconnect bypass fraud within a public switch telephone network (PSTN). In this instance, fraudulent actors route calls through OTT VoIP clients (in a similar fashion to how SIMbox interconnect works, again disrupting termination fee payments), by terminating the calls to end users who have the OTT VoIP app installed on their phone. At no point in this process does either party - neither the person initiating the call, nor the person answering it - know that the call has been intercepted by a third party to be re-routed. This means that the person making the call from a regular telephone doesn't know that it has been switched to a VoIP app, and the person receiving it on a VoIP app doesn't know that it was initiated from a regular phone.

That the call is intercepted without either party's knowledge represents a significant security and privacy risk for subscribers, as they have no visibility into who may be monitoring and tracking their calls. Because the call is routed through a PSTN to OTT VoIP Gateway, privacy is compromised at massive scale and opens the door to further fraud and security risks.

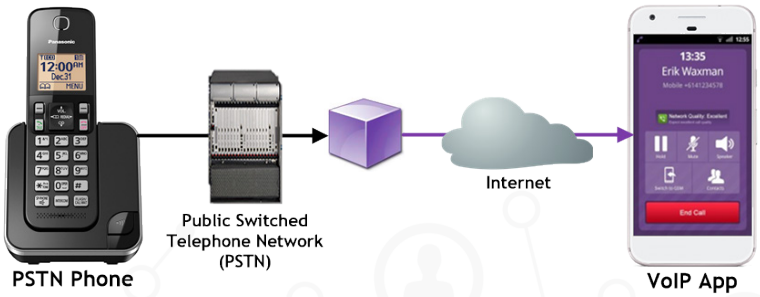

Figure 3 - OTT Voice Bypass Fraud Call

2. More details on SIMbox fraud: https://en.wikipedia.org/wiki/SIM_box

OTT Voice Bypass Fraud Investigation

Because of Sandvine's experience and expertise in recognizing OTT applications, several Sandvine customers asked us to investigate just how prevalent OTT Voice Bypass fraud was on their network.

To research this subject, we examined calls from a leading OTT VoIP app known to be used to commit OTT Voice Bypass fraud. We refer to this app as "OTT VoIP app X.

By using the advanced heuristics and machine learning capabilities of the Sandvine platform, we were able to differentiate between OTT VoIP app X to OTT VoIP app X calls (Figure 2) from fraudulent OTT VoIP app X "In Calling"calls (Figure 3).

With this understanding of varying call types, Sandvine used our business intelligence solutions to break out the composition of OTT VoIP app X. These visualizations made it easy to understand how much direct OTT VoIP app X calling and how much OTT VoIP app X "In Calling" traffic was on the network.

Figure 4 shows that based on observations at this one CSP, after the ability to separate calls that use the "In Calling" feature of VoIP app X, it was revealed that "In Calling" is regularly responsible for over 60% of the OTT VoIP app X's total traffic on this network.

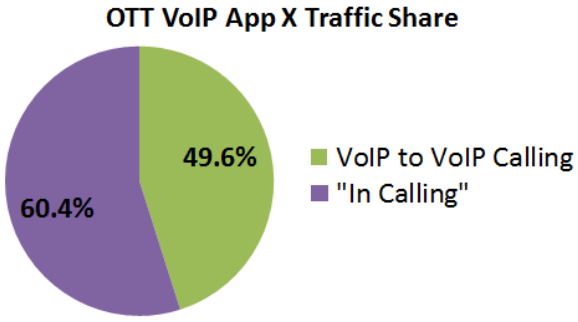

Figure 4 - OTT VoIP App X Traffic Share

Calculating Lost Revenues

Since voice interconnect fees are typically billed by the minute, it is important to try and understand how many minutes of OTT VoIP app X "In Calling" calls were seen in this network during the investigation period so that potential lost revenues could be calculated. After internal research on bitrates of OTT VoIP app X, we concluded that on a monthly basis, more than five million minutes of "In Calling" calls are being terminated on this sample emerging market network.

Since the origin country of each international call is impossible to determine, calculating an exact total of lost revenue from termination fees for this particular study proved to be a challenge. Many calls could be from local networks, or from networks with lower termination rates. When looking at public sources for termination fees, a 2014 report from the Organisation for Economic Co-operation and Development (OECD)[3], showed that the average termination fee for a call from the United States to the country where this network is located was over $0.20 USD per minute. Using this termination rate as a rough baseline for international calling, Sandvine estimates that with the five million OTT VoIP app X minutes observed, this CSP is likely losing hundreds of thousands of dollars each month, and potentially millions of dollars each year to OTT Voice Bypass fraud.

How Can Operators Stop OTT Voice Bypass Fraud?

OTT Voice Bypass Fraud is a growing fraud field, for which few solutions have been brought to market. Many operators are likely to view this type of activity as both a source of revenue leakage and a security/privacy risk for their subscribers. Regulators and Subscribers will certainly be mostly concerned about privacy and security threats posed by the use of these bypass techniques. Unlike SIMbox fraud, Sandvine believes that OTT Voice Bypass fraud can be measured and analyzed through network policy control solutions that have a deep understanding of IP networks, and the ability to intelligently and accurately detect OTT VoIP applications (even encrypted applications - which calls for the use of advanced traffic identification techniques, like machine learning). This knowledge will equip all stakeholders involved in making the appropriate decisions to deal with the impacts according to the local regulatory and legal frameworks.

3. OECD (2014), "International Traffic Termination", OECD Digital Economy Papers, No. 238, OECD Publishing.DOI: 10.1787/5jz2m5mnlvkc-en

Headquarters
Sandvine Incorporated ULC
Waterloo, Ontario Canada
Phone: +1 519 880 2600
Email: sales@sandvine.com

sandvine®
Intelligent Broadband Networks