**Contribution Title:** Edits to section 5 of CPAS-LT white paper

**Source:** Jim McEachern, ATIS, jmceachern@atis.org

**Abstract:** The ATIS TOPS Council Calling Party Anti Spoofing Landscape Team (CPAS-LT) is drawing on the technical work of NGIIF and PTSC to produce a white paper on anti-spoofing mechanisms, aimed at a regulatory audience. IP-NNI Task Force input is requested to validate the proposed text describing calling scenarios.

Section 5 of the CPAS-LT white paper describes the scenarios for call origination, call termination, and network intermediates. However, it treats each category separately, and does not discuss the large number of combinations that are possible. This contribution proposes the addition of diagrams and text to clarify this.

**ATIS-0x0000x**

**A Summary of Calling Party Spoofing Mechanisms and Mitigation Techniques**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

Abstract text here.

## Calling Scenario Examples

The range of possible calling scenarios in the above sections can be illustrated with the following diagram. Reality is actually far more complex than this diagram suggests, with many suppliers providing the equipment within each category shown below, and different software releases, with different functionality, for each supplier’s equipment. In addition, in many cases the equipment has been manufacturer-discontinued, or the supplier is no longer in business.



Although this diagram is a simplification of the range of calling scenarios found in today’s network, it is close enough to illustrate the limitations of simplistic approaches claiming to “solve” the problem of caller-id spoofing.

As terminating service providers consider mechanisms to stop unwanted calls, and in particular as they investigate “Caller-id spoofing” mitigation techniques, their options are limited by the fact that they do not have an end to end view of the full path of the incoming call. As a result, they do not have reliable information on where the call originated, and do not have any information that would allow meaningful estimates of the accuracy of the calling party information in the call signaling. This can be illustrated by the following diagram showing the terminating service provider’s view of an incoming call.



The terminating service provider knows that an incoming call is coming from an intermediate service provider, over an IP connection with SIP signaling, but that is all it can see. If the picture is expanded to show some of the possible sources of this incoming call, a far more complex picture emerges.



The inability of the terminating service provider to have any knowledge of the source of a call complicates attempts to mitigate caller-id spoofing and makes it impossible to rely on the accuracy of the incoming calling party information. This undermines the effectiveness of mechanisms intended to stop malicious calls.

Key insights emerge if one views this from the perspective of a con man, spoofing the caller-id to convince you a call is from the IRS. Today, an abundance of tools are available to spoof the caller-id. It has been suggested the best strategy is to identify today’s dominant weak spot, and develop a targeted “solution” – a “silver bullet”. The International Gateway is sometimes identified as the critical weak link in the existing system, and it has been suggested that addressing that weakness will “solve the problem”. The following diagram illustrates some of the limitations of a simplistic approach like this.



This illustrates that the “international gateway problem” is not in fact just one “problem”, since international gateway traffic can enter the network in many ways. Mandating a solution to block one of these routes, would simply shift traffic to other approaches, including new methods not shown here.

The challenges can also be illustrated by examining one of the more complex scenarios today, where an international gateway is “hidden” behind an enterprise Asterisk PBX, as shown below.



This diagram illustrates some of the points in this traffic flow where problems with calling party mitigation techniques occur today:

1. When traffic is passed from the intermediate service provider to the terminating service provider, no mechanism is defined to identify if calling party information has been validated, or the source of the information. The only information available is whether or not the service provider is “trusted”. Potential solutions are being developed for SIP signaling, but nothing exists or could be developed for TDM traffic.
2. When traffic is passed from the originating service provider to the intermediate service provider, no mechanism is defined to identify if calling party information has been validated, or the source of the information. The only information available is whether or not the service provider is “trusted”. Potential solutions are being developed for SIP signaling, but nothing exists or could be developed for TDM traffic.
3. In the future, mechanisms may be defined to indicate that the calling party information has been validated, but if that traffic originated in a TDM/SS7 network, it is impossible to obtain reliable information about the origination point. The end-to-end information is limited by the SS7 network, even though most of the signaling path is via SIP.
4. Today, calling party information is inserted by the PBX and is not validated by the network. In the case of TDM equipment, it would be impossible to change this since the majority of the equipment is no longer supported by the manufacturer.
5. The ultimate source of the traffic may be an “international gateway” that is “hidden” behind an enterprise PBX. The nature of equipment such as an Asterisk PBX makes it very inexpensive to integrate international gateway functionality into the PBX and create new entry points for malicious traffic. The service provider does not have any mechanism to stop, or even to detect, this situation.

As this example makes clear, addressing the challenges of calling party spoofing requires an end-to-end perspective that addresses a wide range of service providers, equipment, and functionality.

Calling party spoofing is not a single, well-defined problem that can be addressed with a single “silver-bullet solution”. It’s helpful to use the analogy of a flood to better understand the situation. If the problem is a single leak in the dyke, one small finger is enough to stem the flow. But if a sieve is the only thing holding back the flood, clearly a different approach is required. A realistic strategy must address specific threats where practical, but must also take a layered approach that adds secondary defenses to minimize the impact when even the best defense is inevitably bypassed. The strategy must also recognize that the threat is not static. As one threat vector is blocked, the attacks will shift to other weak points, and even discover new approaches that do not yet exist. Effective mechanisms to mitigate calling party spoofing must recognize this reality, and be structured accordingly.