SIPPING Working Group	S. Niccolini
Internet-Draft	J. Quittek
Intended status: Informational	J. Seedorf
Expires: August 18, 2008	NEC
	February 15, 2008

TOC

Signaling TO Prevent SPIT (SPITSTOP) Reference Scenario
draft-niccolini-sipping-spitstop-01

Status of this Memo

Abstract

This memo discusses the need for standards that support SPam over Internet Telephony (SPIT) prevention applications. After explaining the general need for SPIT prevention applications the memo provides a reference scenario for potential communication between entities that may be involved in SPIT prevention. Within this scenario the need for standardizing communication is analyzed for each pair of communicating entities. The analysis is intended to serve as a starting point for discussing the requirements for signaling standards as well as for architectural considerations, that support SPIT prevention applications.
This memo is not intended to suggest any solution of SPIT signaling issues. Such work, if necessary at all, should be object of separate documents.

Table of Contents

---

1. Introduction

TOC

Email is an essential mean for world-wide communication. The openness of the Internet make use of email easy but also makes it easy to mis-use it, particular to annoy users with spam email. Today, there is more spam email transmitted by the public Internet than regular email. Internet telephony is on its way to replace the traditional circuit-switched telephony. There is a strong concern that this migration to the open Internet will result in Spam over Internet Telephony (SPIT) that potentially will be annoy the users even more than spam email does today. If there are more SPIT calls than regular calls in the telephony world, then phones will ring all day making it hard to use this medium in a convenient and productive way.
This memo discusses the need for producing standards that help preventing SPIT in the future. Although SPIT is not an actual problem today, it has a big potential to become one very soon. At this point in time it will be good to be prepared and have technology already available that protects users from SPIT.

1.1. The SPIT Threat

TOC

Most of the spam emails are generated by so-called bot nets. Bot nets are networks of hosts that have been invaded by a spammer in order to use them for sending spam email without the knowledge of or admission by the regular administrators of these hosts. Bot nets can easily be used for initiating spam voice calls instead of or in addition to sending spam email.

Today, there is already voice spam in the switched telephony network. Many households in Europe receive between 1 and 10 automated spam calls per month. During such a call, a prerecorded messages is played to the callee without supporting any interaction. However, these calls create significant cost for the caller, at least if they are made in numbers of thousands or hundred thousands.

With the ongoing migration from traditional connection-switched telephony to packet-switched Internet telephony the cost of spam calls will drop drastically. The infrastructure for generating Spam over Internet Telephony (SPIT) is already there in form of the existing bot nets. A recent study [RFC5039] (Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," January 2008.) estimated that the cost per delivery of SPIT call will be up to four order of magnitude cheaper than the costs per delivery of spam over circuit-switched telephony. This is expected to cause a flood of SPIT calls as soon as Internet telephony becomes the dominating telephony technology. For dealing with this problem, particularly for preventing unwanted SPIT, not all methods that are used today for blocking spam email can be applied. Particularly, content checking, that is a basic method for detecting email spam, is not applicable, because content of a call is not available for checking before the phone rings. And stopping the phone from ringing for spam calls is one of the major goals of SPIT prevention. Therefore, further methods are needed. An overview of methods that are currently available for SPIT prevention is given in [RFC5039] (Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," January 2008.).

The number of SPIT prevention methods listed there is quite large. Still, it is not considered to be a complete list or a list that is exhaustive enough for preventing SPIT sufficiently. On the contrary, this list shows that there are still a lot of opportunities left for SPIT generators to place SPIT calls successfully.

1.2. Communication Need for SPIT Prevention

TOC

An important aspect in this context has not been investigated in detail yet. It is sharing of information between entities that are involved in preventing SPIT. They may have a need to exchange information related to SPIT. The range of information to be exchanged includes information about

*SPIT events that actually occurred,

*indicators concerning callers to be sources of SPIT,

*indicators concerning concrete calls to be SPIT,

*etc.

This memo investigates the need of communication between entities involved in SPIT prevention and the need of standards for this communication. For this purpose, a reference scenario is defined in Section 2 (Reference Scenario) that serves for identifying which communications interfaces may be required for sharing SPIT-related information between involved entities. Based on this scenario, requirements for individual interfaces are discussed in Section 3 (Signaling Interfaces Considerations).
Currently, the requirements are stated on a high level. Future revisions of this memo may elaborate the requirements in more detail. Which (kind of) communication protocol should be chosen for meeting the requirements is not subject of this memo.
However, this memo is supposed to stimulate discussion on the need of standardization work in this area. The standardization work should both identify the reference architecture, the best suited protocols for such information sharing at each interface and if extensions to such protocols for the support of SPIT information sharing is needed. If no suitable protocols matching the requirements for a particular interface is found a suggestion for the design of a new protocol suited to such information sharing should be initiated.

---

2. Reference Scenario

TOC

For our reference scenario we consider four kinds of communicating entities:

*the caller User Agent (UA) that generates SPIT,

*Proxy Servers (PS) forwarding call signaling,

*specialized SPIT prevention entities,

*the callee User Agent (UA).

With the goal of avoiding that the callee's phone rings for SPIT calls, SPIT prevention devices should detect a SPIT message already based on the INVITE method that is sent in order to initiate the SPIT call. This goal can only be achieved along the path the INVITE message is forwarded from the caller towards the callee. This path starts at the caller UA, then potentially includes a set of forwarding PS, and terminates latest at the callee UA.
Please note that the described reference scenario can be easily mapped to the framework overview described in [I-D.tschofenig-sipping-framework-spit-reduction] (Tschofenig, H., Schulzrinne, H., Wing, D., Rosenberg, J., and D. Schwartz, “A Framework

to tackle Spam and Unwanted Communication for Internet Telephony," July 2008.), the major difference is that the framework discussed in such a draft takes into account only one domain boundary while the reference scenario here described is more general and assumes that interactions among multiple domains could be used in order to allow distributed decisions.

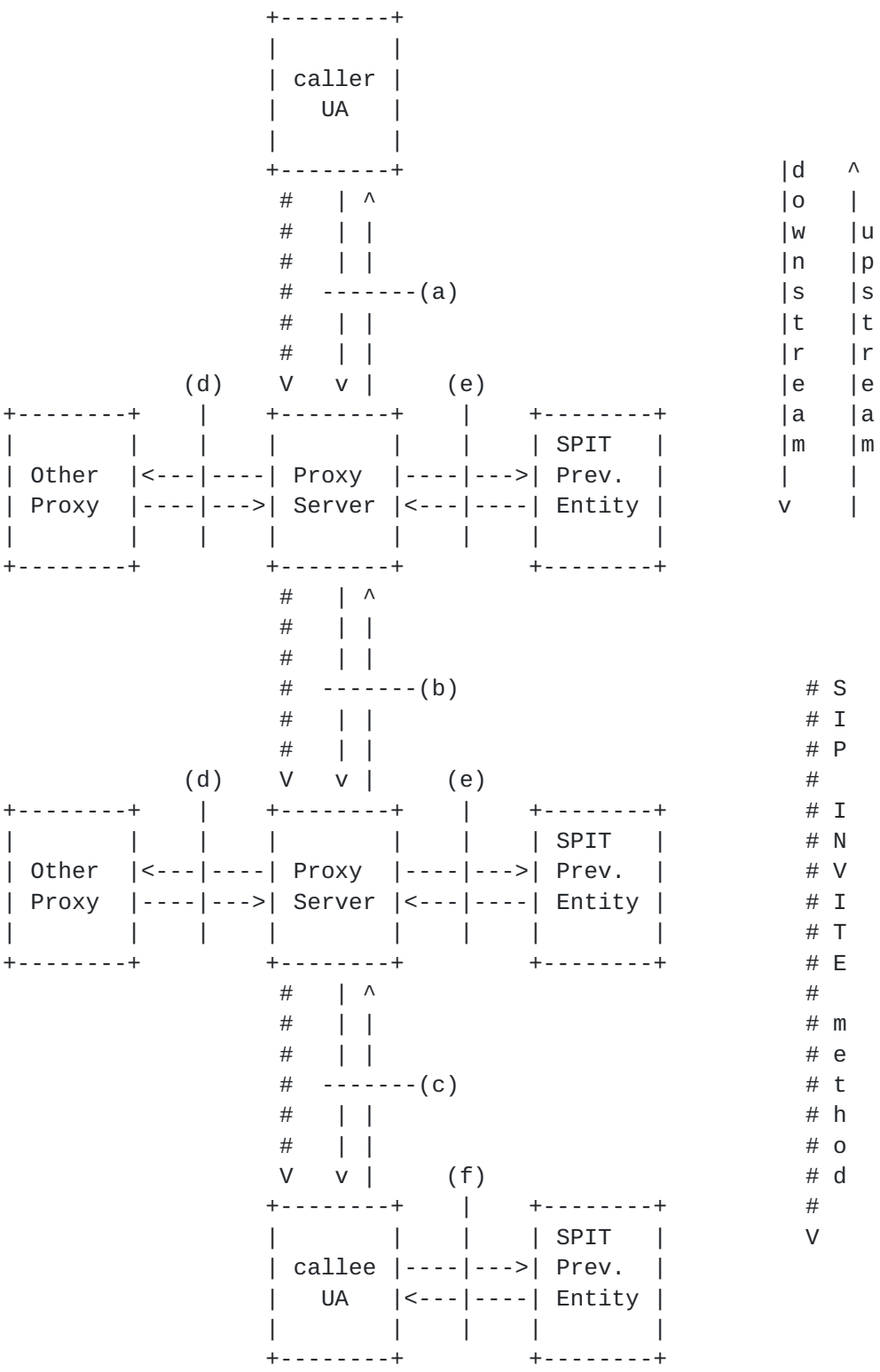

Figure 1: SPIT prevention reference scenario with two proxy servers

Entities on the path from caller to callee may share information related to SPIT prevention. Related communication may happen already before a certain INVITE methods is transmitted or it may be initiated by this message. If this communication includes transmitting information in the same direction as the INVITE message along the path, then we talk about downstream communication. Transmitting information in the opposite direction we call upstream communication.
The SPIT prevention reference scenario shown in Figure 1 (SPIT prevention reference scenario with two proxy servers) contains a caller UA, a callee UA and two PS on the path of the INVITE message from caller UA to callee UA. This number of PS was chosen because it contains exactly one instance of each pair of interacting kinds of entities along the path of the INVITE message:

- at interface (a) the caller UA is interacting with a PS,
- at interface (b) two consecutive PS are interacting with each other,
- at interface (c) a PS is interacting with the callee UA.

The number of two PS matched the common SIP signaling trapezoid. However, any number of proxy servers greater than zero can be applied to the scenario. If there is only one PS present, then the interface (b) is not instantiated. If there are two or more PS on the path, then interface (b) is used between each consecutive pair of them. In general, the INVITE message could be sent directly from caller UA to callee UA without involving any PS. A direct call would be possible if the caller UA sends the INVITE directly to the callee UA, anyway such IP address retrieval is prone to errors either because of possible change of IP address during time of callee UA or because of Network Address Translator along the path masking the real IP address. The direct call case becomes even less relevant if the callee UAs are configured to accept INVITEs only from their proxy servers. For these reasons we decided not to include an interface for direct communication between caller UA and callee UA in the reference scenario.
Each proxy server on the signaling path of the INVITE message may communicate with off-path entities in order to help the task of SPIT identification and prevention.
These entities include one or more specific SPIT prevention entities that are consulted by the proxy server using interface (e) in order to get an indication or estimation of a given INVITE message to belong to a SPIT call (e.g. using authorization policies).
These entities also include one or more cooperating PS with which information about SPIT calls (or call attempts) is shared using interface (d) in order to improve the SPIT prevention accuracy. An example for such a cooperation would be a set of PS in a single administrative domain sharing information about known sources of SPIT (federation of black listing services across PS).
The callee UA may also interact with a specific SPIT prevention entity similar to the PS (e.g. a local one located near the user agent in the access domain). Since in this case, the offered service might be more

personalized than in the case of the PS, we use a different interface (f) for our reference model. This does not preclude that instantiations of (e) and (f) may have identical functions (e.g. using the same authorization policies language [I-D.tschofenig-sipping-spit-policy] (Tschofenig, H., Wing, D., Schulzrinne, H., Froment, T., and G. Dawirs, "A Document Format for Expressing Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony," July 2008.)).

---

3. Signaling Interfaces Considerations

TOC

This section discusses the interactions between entities of the reference scenario that is shown in Figure 1 (SPIT prevention reference scenario with two proxy servers). The interfaces are grouped into three sections.

1. The first one deals with interfaces (a), (b), and (c) which all serve for exchanging information between consecutive entities along the path of the INVITE message of a particular call (e.g. spam scores or spam feedbacks with well defined semantics).

2. Interface (d) has a similar function but is off-path and not necessarily related to individual (SPIT) calls (e.g. black listing services across PS).

3. Interfaces (e) and (f) are used by PS or the callee UA when they need to decide whether or not to consider a particular call request as SPIT (e.g. authorization policies).

3.1. Interfaces on the Signaling Path

TOC

At all three interfaces (a), (b), and (c) information may be exchanged in upstream direction as well as in downstream direction.

3.1.1. Downstream

TOC

There are several considerations of downstream communication that apply to all three interfaces. We first describe them before pointing out differences between the three interfaces.

> **All Interfaces (a), (b), and (c)** Downstream information is sent along with an INVITE in order to provide information about the INVITE to belong to a SPIT call (e.g. indicate that a caller is exceeding a sending treshold, that the caller did not pass a specific test like a CAPTCA test , etc.). A sender or forwarder

of an INVITE may, for example, want to signal such information to the downstream entity (be it PS or UA) but still not have sufficient certainty or not have legal rights for blocking a SPIT call.

In any case, interface (a), (b), or (c) would allow to pass such information further along the path of the INVITE. Even if such information does not always lead to achieving a clear idea on the nature of the requested call (e.g. the final decision is taken only by downstream entities, like the UA), the transmitted information can be recorded by the receivers of this information and used for improving future judgments of call requests for SPIT prevention.

In addition such interfaces would allow to pass statistics about the recent behavior of the sender. An example of these statistics would consist in the rate of (SPIT) calls initiated by the sender during the last time slot, the ratio between regular calls and SPIT calls initiated by the sender during the last time slot, etc. The above mentioned statistics can also be bundled together and passed only after the expiration of a timeout in order to increase scalability.

Besides the estimation and the statistics itself, also the source of the estimation may be transmitted. This way, an entity can indicate, whether it has been involved in producing the estimate, or just forwarded the received estimation along the path of the INVITE.

Interface (a) This interface is instantiated between the caller UA and the first PS along the INVITE path. The relevance of interface (a) seems to be rather limited. It does not seem a good idea to have the caller UA neither estimating itself the likelihood of the INVITE to belong to a SPIT call not transmitting statistics about the its recent behavior. Moreover the instantiation of such an interface could be maliciously used by entities initiating SPIT without the PS having the proper means to judge if the information passed is trustable or not.

Interface (b) This interface is instantiated if there are two or more PS on the path. In this case interface (b) is used between each consecutive pair of them. It is used to send downstream information about the infomration associated with an INVITE (e.g. the caller has a bad reputation according ot the originating domain) and about most relevant statistics of the INVITE initiator recent behavior. If also the source of the estimation and statistics is transmitted, a receiving PS may be able to judge how much trust to associate with the indications based on local policies. Still depending on local policies and legal rights the PS can decide to carry out additional tests on the INVITE, initiate communication to other entities (see Section 3.2 (Off-Path Interfaces between Proxy Servers) or Section 3.3

(Interfaces to Special SPIT Prevention Entities)), or block the call.

Interface (c) This interface is instantiated between the last PS and the callee UA. It is used to send downstream information about the information associated with an INVITE (e.g. the caller did not pass a CAPTCHA) and about most relevant statistics of the INVITE initiator recent behavior. If also the source of the estimation and statistics is transmitted, the callee UA can judge how much trust to associate to the indications based on local policies. Still depending on local policies and legal rights the callee UA can decide to carry out additional tests on the INVITE, initiate communication to other entities (see Section 3.3 (Interfaces to Special SPIT Prevention Entities)), or block the call without having the phone ringing.

3.1.2. Upstream

TOC

As for downstream communication above, we first describe considerations that are common for all three interfaces before them before pointing out differences between them.

All Interfaces (a), (b), and (c) Upstream information is sent by entities after receiving an INVITE as feedback to the entity from which they received it. It may contain a feedback on the INVITE received. This feedback may be sent before the call is established (if at all), after it was blocked, while the call is established, and after the call has been terminated. This information can help the sender in better judging following calls that are forwarded and the users sending the call initiation request or to block subsequent calls of the same caller for the callee (feedback to insert users in black lists hosted at the PS). An example for the delivery of feedback information is reported in separate documents .

In addition to the feedback associated to a particular INVITE, such interfaces, similar to downstream communication of statistics, would allow to feed back statistics about the recent behavior of the sender. An example of these statistics would consist in the rate of SPIT calls (estimated using the feedback mechanism) initiated by the sender during the last time slot, the ratio between regular calls and SPIT calls initiated by the sender during the last time slot, etc. The above mentioned statistics can also be bundled together and passed only after the expiration of a timeout in order to increase scalability.

Similar to downstream communication of information and statistics, the source of the feedback information may be

contained. This is particularly interesting if the feedback was generated by the callee who received the call.

Interface (a) This interface is instantiated between the first PS along the INVITE path and the caller UA. The relevance of interface (a) seems to be rather limited. It does not seem to be a good idea to give feedback to an initiator of SPIT on if and why requested calls have been blocked. This would allow the SPIT initiator to use this feedback for improving methods that bypass SPIT prevention systems in the network.

A potential argument for sending a notification about detected SPIT to the SPIT generator would be that many legal operators of SPIT generating hosts might not be aware of this. Today, this is the case for email spam. Most of them are generated by bot nets where the legal operators of the contained hosts are not aware of their hosts being used for this purpose. However, in case of SPIT generation, it must be assumed that the generating software is either a software not in control of the legal operator or it is controlling the caller UA and capable of suppressing any feedback that should not be seen by the legal operator. Therefore, this means would probably not show the desired results.

Interface (b) This interface is instantiated if there are two or more PS on the path. In this case interface (b) is used between each consecutive pair of them. It is used to feed back information about a certain INVITE (e.g. callee indicated the call as SPIT) and about most relevant statistics of the INVITE initiator recent behavior. If also the source of the information and statistics is transmitted, the PS can judge how much trust to associate to the indications based on local policies and act consequently. Still depending on local policies and legal rights the PS can decide to carry out additional tests on selected subsequent INVITEs, initiate communication to other entities (see Section 3.2 (Off-Path Interfaces between Proxy Servers) or Section 3.3 (Interfaces to Special SPIT Prevention Entities)), or block selected subsequent calls.

Interface (c) This interface is instantiated between the callee UA and the last PS along the INVITE path. It is used to feed back information about an INVITE (e.g. it belonged to a SPIT call) and about most relevant statistics of the INVITE initiator recent behavior (even if in this case the statistics can be rather limited since are generated by the callee UA directly which has a narrow view on all the traffic). This feedback is supposed to be a very important one since it is the one directly generated by the callee UA (be it the software or the human itself). The PS will therefore associate high trust to such a feedback and act consequently. Still depending on local policies and legal rights the PS can decide to carry out additional tests on selected subsequent INVITEs, initiate communication to other entities (see Section 3.2 (Off-Path Interfaces between Proxy Servers) or

> Section 3.3 (Interfaces to Special SPIT Prevention Entities)), or block selected subsequent calls.

3.2. Off-Path Interfaces between Proxy Servers

TOC

The basic idea of interface (d) is similar to the interface (b) where different PS exchange SPIT-related information. The difference to (b) is that for (d) this exchange is not bound to the path of an INVITE message. At interface (d) information will be shared among PS that collaborate on SPIT prevention (e.g. federations). While the (b) interface can potentially be an inter-domain interface, (d) is rather seen as an intra-domain interface where collaborating proxies of a domain enforce a domain-wide SPIT prevention policy. For such a purpose, information needs to be exchanged rather on collected information than on single events of an observed INVITE message, although this case should not be excluded.
Interface (d) has two major purposes. the first is the exchange of information regarding certain caller UAs or certain administrative domains estimated to produce SPIT. This does not necessarily require exchanging observations per INVITE message, but rather on a regular basis or incident-driven, for example whenever a PS detects a correlation between several calls that have been classified as SPIT. The exchange of such information may, for example, lead to a classification of a source address or a source network as source of SPIT which requires and update of blacklists and SPIT detection mechanisms.
Consequently, the second major purpose of interface (d) is exchanging information that updates or synchronizes the prevention mechanisms that are acting at different PS. This includes particularly blacklist and whitelist entries, but also other SPIT prevention mechanisms may make use of exchanged information.
Still, interface (d) may also serve for exchanging estimated results associated to single calls, for example for collecting this information at a central repository that serves for updating domain-wide SPIT prevention policies.

3.3. Interfaces to Special SPIT Prevention Entities

TOC

Communication to special SPIT prevention entities can be performed either by a proxy server via interface (e) or by the callee UA via interface (f). We first discuss considerations that apply to both interfaces before pointing out differences between the two.

> **Both Interfaces (e) and (f)** The service offered by special SPIT prevention entities is related to the estimation of an INVITE to belong to a SPIT call. This communication is supposed to be

instantiated in order to off-load computational intensive tasks to an external entity.

The communication with this SPIT prevention entity follows the client-server scheme. The PS or UA acting as client requests an estimation for a given INVITE message to belong to a SPIT call. The estimation is performed by the SPIT prevention entity acting as server. A request may include call parameters to be used by the server when performing the estimations.

Interface (e) This interface is instantiated between a proxy server and a special SPIT prevention entity in order to request for SPIT estimations. In addition to the above considerations it is necessary to note that such service could be less personalized with respect to the service offered over the interface (f) since the estimations have to be general in order to deal with all the users served by the proxy server using such an interface. Otherwise the instantiated functions seems to be identical.

Interface (f) This interface is instantiated between a UA and a special SPIT prevention entity in order to request for SPIT estimations. In addition to the above considerations it is necessary to note that such service should be more personalized with respect to the service offered over the interface (e) since the estimations have to be specific to the callee requesting them over the interface. Otherwise the instantiated functions seems to be identical.

---

4. Need for Standardization

TOC

The considerations above indicate that there is an actual need for standardization of communication information.
The strongest need seems to be for interfaces (b) and (c) in upstream direction for providing feedback on calls or call attempts. But also in downstream direction, there seems to be an obvious need to support this communication by providing a standard for it. This concerns both in intra- and inter-domain communication.
The situation is very different for Interface (a). The considerations in Section 3.1 (Interfaces on the Signaling Path) indicate that it might even be a bad idea to provide any feedback via (a) at all. Therefore, we do not see a need to work on standards for interface (a).
Interface (d) seems to be useful but with a more limited scope of application within a (federated) administrative domain (intra-domain). Still for interoperability between different devices it appears to be beneficial to have a standard way of sharing SPIT-related information.
For the remaining interfaces (e) and (f) we do not yet see a clear need for interoperability. SPIT prevention engines to which functions are outsourced by a PS or callee UA may typically be part of a solution that is offered together with the PS or with a set of SIP UAs. For

these cases proprietary communication protocols appear to be sufficient. Still need for standardization may arise at later stages when SPIT prevention entities become more common.

4.1. Preliminary Protocol Considerations

TOC

The fact that the communication over interfaces (b) and (c) follows the same path as the SIP signaling itself may influence the choice of the signaling protocols used for exchanging information at the interfaces. An obvious choice to be discussed would be embedding the SPIT information directly in the SIP messages flowing among the entities anyway.
For the other interfaces (d), (e) and (f) other signaling protocols may be preferable since the communication will happen anyway not synchronously with the SIP messages used to initiate the session. An example could be the exchange of XML files among different entities.

---

5. Conclusions

TOC

This memo addresses the necessity of providing standards for communication between entities involved in SPIT prevention. For this purpose a reference scenario is defined with involved entities and interfaces between them. For each interface the need for it and the need for standards for is discussed.
This memo is intended to stimulate a discussion on SPIT prevention and to reach consensus on the identification of standardization goals and reference architectures in this area. Some of the considerations in Section 3 (Signaling Interfaces Considerations) seem to indicate that there is an actual need to standardize communication for some of the discussed interfaces. This memo does ot try to standardize any solution to the problems identified. The necessary work outcoming from the discussion stimulated will have to be carried out in separate documents.

---

6. Security Considerations

TOC

This memo discusses the exchange of information related to SPIT prevention. This includes information on particular calls or call attempts as well as information on call initiators potentially being a source of SPIT.
Exchanging per-call information may violate the privacy of a caller. Therefore, instantiations of the discussed exchange of information need to be carefully checked for compliance with legal regulations of information privacy. Also, since this information may be sensitive,

appropriate steps should be undertaken to provide confidentiality when it is transmitted over the Internet.
Both, per-call information and information of a caller being a source of SPIT may be a target of denial-of-service attacks. If such messages are faked, a regular caller may be blocked network-wide and not able anymore to perform calls. Therefore, integrity and authenticity need to be provided when this kind of information is transmitted over the Internet.

---

7. IANA Considerations

TOC

This document has no actions for IANA.

---

8. Informative References

TOC

[RFC5039]	Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam," RFC 5039, January 2008 (TXT).
[I-D.tschofenig-sipping-framework-spit-reduction]	Tschofenig, H., Schulzrinne, H., Wing, D., Rosenberg, J., and D. Schwartz, "A Framework to tackle Spam and Unwanted Communication for Internet Telephony," draft-tschofenig-sipping-framework-spit-reduction-04 (work in progress), July 2008 (TXT).
[I-D.tschofenig-sipping-spit-policy]	Tschofenig, H., Wing, D., Schulzrinne, H., Froment, T., and G. Dawirs, "A Document Format for Expressing Authorization Policies to tackle Spam and Unwanted Communication for Internet Telephony," draft-tschofenig-sipping-spit-policy-03 (work in progress), July 2008 (TXT).

Authors' Addresses

TOC

	Saverio Niccolini
	NEC Laboratories Europe, NEC Europe Ltd.
	Kurfuersten-Anlage 36
	Heidelberg 69115
	Germany
Phone:	+49 (0) 6221 4342 118
Email:	niccolini@nw.neclab.eu
URI:	http://www.nw.neclab.eu
	Juergen Quittek
	NEC Laboratories Europe, NEC Europe Ltd.
	Kurfuersten-Anlage 36

	Heidelberg 69115
	Germany
Phone:	+49 (0) 6221 4342 115
Email:	niccolini@nw.neclab.eu
URI:	http://www.nw.neclab.eu
	Jan Seedorf
	NEC Laboratories Europe, NEC Europe Ltd.
	Kurfuersten-Anlage 36
	Heidelberg 69115
	Germany
Phone:	+49 (0) 6221 4342 221
Email:	seedorf@nw.neclab.eu
URI:	http://www.nw.neclab.eu

Full Copyright Statement

TOC

Intellectual Property