# Advanced Consideration of a Caller Pre-Validation Against Direct Spam Over Internet Telephony

Jürgen Müller and Michael Massoth
Department of Computer Science
Hochschule Darmstadt University of Applied Sciences
Darmstadt, Germany
e-mail: {juergen.mueller, michael.massoth}@h-da.de

***Abstract*—Spam over Internet Telephony as the distribution of unwanted voice messages over Voice over Internet Protocol networks is an upcoming threat. It is harder to prevent than e-mail spam since its content is not available before the victim is annoyed. This is even more difficult if the spam is sent directly to the victim's user equipment, bypassing the proxies of the service provider. Hence, this messages cannot be filtered, since the proxies are no longer participating in the transaction. This article presents a pre-validation mechanism, which ensures a minimum level of trust about the caller. It assumes that a legal registered user does not send any spam, since his service provider will penalize him if he does so. Therefore, the pre-validation mechanism sends some requests to the presence server of the provider and the user equipment of the caller to validate their existence. This enables the knowledge to allow a call attempt of an unknown user.**

***Index Terms*—Communication system security; Telephone equipment; Telephony; Spam**

## I. Introduction

Spam over Internet Telephony (SPIT) is an upcoming problem in the internet and telecommunication society. This section gives a brief overview on SPIT. A lot of groups are affected. There are individuals and companies that use Voice over Internet Protocol (VoIP) because it is cheap. Additionally, there are spammers who want to send unsolicited calls.

Regarding a study of the German Federal Office for Information Security, about 98.5 % of e-mails received in Germany in 2008 were spam [2]. It would not be possible to use VoIP properly if this amount of spam would arrive in the VoIP networks. However, it is not described clearly if the whole 98.5 % are spam or unwanted e-mails in general.

The MessageLabs Intelligence Reports provides on a monthly basis the latest thread trend, including the spam propagation [3]. Therefore, the e-mail spam rate in the last 18 month was in an average on a level of about 90.5 %, as depicted in Figure 1.

In addition to annoyance, there is a big problem with cost caused by spam. According to a prediction of Ferris Research, the worldwide cost for spam grew up to $130 billion in 2009 [4].

A new kind of view on the spam phenomenon is given in a report by McAfee [5]. The authors describe herein that the whole amount of annual spam leads to a power consumption of 33 billion kilowatt-hours. That amount corresponds to the electricity used in 2.4 million homes in the United States of America.

VoIP has been designed to reduce telephony-related cost. First of all, providers want to save money, but this means a reduction of cost for spammers as well. Sending spam via internet telephony is much cheaper than sending it by a public switched telephone network.

Indeed, the distribution of e-mail spam is cheap as well. However, there is a major advantage of SPIT over e-mail spam: It is harder to detect. Therefore, more SPIT gets through to a callee than spam e-mails arrive in a mailbox.

The group of victims in addition grows. The number of residential, small- or home office VoIP subscribers grew 24 % in 2009 to 132 million worldwide [6]. 10.3 million of this VoIP users resides in Germany 2010 [7]. In the future, the total number of mobile VoIP users will reach 288 million by the end of 2013 [8].

This article is structured as follows: Section II introduces the process of SPIT and its two types. In Section III, all existing defense mechanisms that could be applicable against SPIT are introduced. The proposed caller pre-validation mechanism is introduced in Section IV. Section V describes how this mechanism could be attacked. Section VI contains a performance analysis of the proposed mechanism. A look forward and an introduction to future improvements are given in Section VII.

## II. Background

It is important to know how SPIT works in order to understand it. As shown in Figure 2, there are three steps [9]. First of all, the spammer needs to collect addresses to send his messages to. The next step is the session establishment. The message itself is sent to the callee in the third step. The most relevant step is the address gathering, because this step enables the attack.


Fig. 2. The three steps of Spam over Internet Telephony [9].

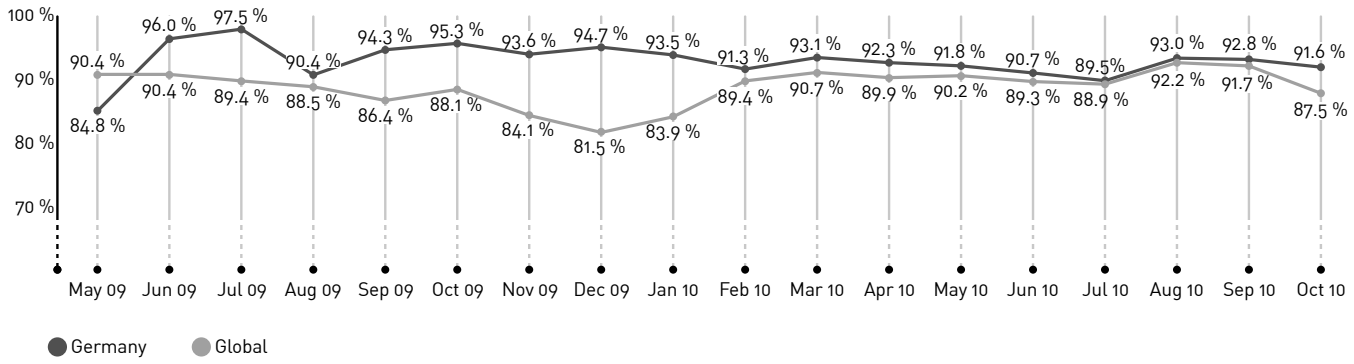


Fig. 1. E-mail spam rate between May 2009 and October 2010 [3].

### A. Gathering Addresses

The question of interest is how spammers are able to acquire these addresses. Surveys show that there are at least five options to achieve this objective [9][10][11]:

- Trading: On the internet, there are several opportunities to buy whole lists of addresses. This is the easiest way to gather addresses.
- Harvesting: Spammers use so-called bots, which are automatically searching for addresses in the internet. This can be done by scanning page code for strings in special syntaxes. For example a SIP URI mainly consists of the sub strings "sip:" and the @-sign. Furthermore, spammers steadily get more addresses just by waiting.
- Active scanning (with permanent SIP URIs): The spammer needs a valid account in the network of the desired provider to launch this attack. However, he has to find out how addresses are put together among this provider. Next, the spammer starts an automated test call to each possible SIP URI. A successful call attempt identifies an assigned address.
- Active scanning (with temporary SIP URIs): This possibility is very similar to active scanning. The difference is that there is no message being sent via the infrastructure of the provider. Instead, they are sent directly to the callee's user equipment. Since spammers do not know the correct domain part of the temporary SIP URI, they have to figure out the range of IP addresses that are assigned by the corresponding provider. So, the spammer has to check each possible combination of user name and IP address.
- Passive scanning: An active scan implies the possibility of detection by a network administrator. Therefore, a spammer can host a web site or hotline and offer, for instance, a value-added service. Each user who wants to use that service has to register himself on the web site or to call a certain hotline. Every number who calls this hotline or is sent via the registration form can be stored for a SPIT attack.

The active scan attack is the most interesting source of addresses. A spammer could achieve three lists during his scan. The first one contains all addresses that are assigned and currently registered, i.e., the addresses that responded with a 200 OK response. A second list contains the addresses that are assigned but currently not registered, i.e., the addresses that responded with a 480 Temporarily Unavailable. The last list holds unassigned addresses that answered with a 404 Not Found response. The last one could be used for future scan attacks.

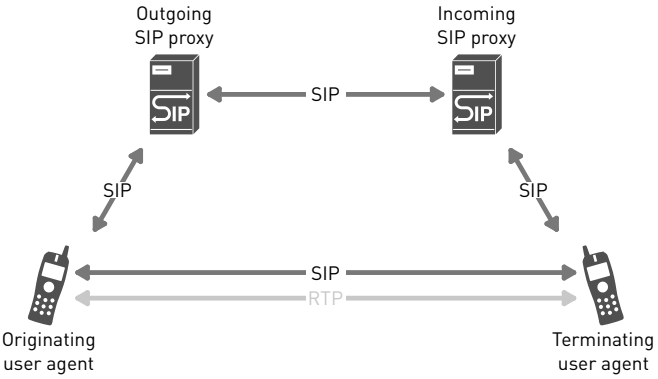


Fig. 3. The regular SIP trapezoid.

### B. Session Establishment

The spammer could start to launch the spam attack itself, as soon as he collected enough addresses. Therefore, he has to establish a connection to each victim. He has two possibilities to establish these connections because he can gain two lists of assigned addresses (i.e., permanent and temporary SIP URI lists) [9]:

- SPIT via Proxy: The spammer uses the permanent SIP URI list to send his messages via the proxies of the provider.
  This so called SPIT via Proxy is the most usual form of SPIT. The messages sent by the spammer first arrive at proxies belonging to the provider, as shown in Figure 3. These proxies are able to take some actions against SPIT and redirect it to its destination.
  The provider is able to challenge the caller before he accepts his messages, too. So, only known and trusted users are able to participate in the system.
- Direct SPIT: A spammer usually does not want that

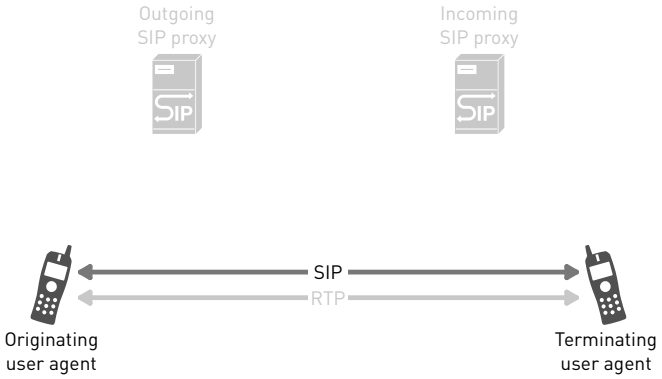


Fig. 4. SIP trapezoid within a direct connection.

his messages are rejected. Therefore, he can use the temporary SIP URI list.

Direct SPIT is a bit different from SPIT via Proxy, as shown in Figure 4. The message is sent directly to the callee's user equipment using the temporary SIP URI.

Where is the disadvantage for a detection system in this case? No proxy is involved in the message flow and no filtering can be applied to the message. Most user equipments are not designed to handle spam by themselves. It is very likely that spammers would use this form of SPIT because of these problems.

This is the reason why Direct SPIT is the most dangerous form of SPIT. A mechanism is needed that is able to analyze the message flow within the user equipment. However, there are only few processing resources in the user equipment for this kind of processing available.

The session establishment in the Direct SPIT scenario is much more dangerous, because no VoIP proxy is involved in this process. Indeed, temporary SIP URIs are only assigned for relatively short periods of time. Therefore, a spammer must possess a very up-to-date list of addresses to perform an attack this way. Nevertheless, a secure mechanism is required to prevent legitimate VoIP users from this attack due to the very high threat of it.

### C. Sending Message

The transmission of the message itself can start after the connection is established. There are multiple possibilities for the sending process, related to the sort of message. They differ in terms of distribution or message type and can be described as follows:

- Call center: A call center consists of several people who talk to their customers personally. The assignment of a call center agent to a customer is usually performed by a computer system. Therefore, it can produce a lot of SPIT. However, such a call center requires a lot of money to operate, because of costs for employees, rooms, and equipment.
- Calling bot: A calling bot is a piece of software that establishes connections to the victims automatically. As soon as the session is built up, a prerecorded message is transmitted, then the session is terminated. It is inexpensive in comparison to a call center, because no staff or large rooms are required. Nevertheless, it is able to distribute a high amount of SPIT.
- Ringtone SPIT: Some user equipments are capable to understand the Alert-Info header field [12] of an INVITE request. It specifies an alternative ring tone to the user agent. The ring tone is referred to with a Uniform Resource Identifier (URI). This URI contains an audio advertisement as an alternative ring tone. Therefore, the callee does not have to accept the call to get the message. His own user equipment starts immediately to play this message to him.

The most problematic SPIT source is a call center, because legitimate call centers exist, too. This legitimate call centers traffic is hard to differentiate from those sent from illegal call centers.

Regardless of the SPIT source, additional purposes are possible. Most SPIT messages are sent with the intent to advertise a product or service. Unfortunately, there is the possibility of a SPIT message with the only aim to disturb the callee. Therefore, all kinds of annoying VoIP calls are considered as SPIT in the scope of this article.

### D. Relevance of Spam over Internet Telephony

To determine the influence of SPIT on networks and society is difficult. Anyway, no empirical survey concerning SPIT exists so far.

One opportunity to find out its influence is to look at the impact of e-mail spam. Regarding to Jennings, costs caused by spam consists of three main components [4]. As depicted in Figure 5, the major component (85 %) is a loss of user productivity. This term refers to all costs, which are caused if an employee is not able to perform his work. An employee has to take a break from his work to check his e-mail account. He has to check each e-mail to be able to delete spam, to look for false positives, etc. Then he has to continue his original work after that, which needs some extra time.

It is highly probable that this will be a major factor regarding SPIT as well. It is even worse than that. An employee has to check his e-mails manually before he loses time of his original work. SPIT disturbs him for each incoming message, because his phone rings automatically.

Additionally, SPIT requires much more network resources than e-mail spam. This is because of the fact that VoIP consumes much more bandwidth than e-mails.

## III. Related Work

There are a lot of techniques that could be applied against SPIT. However, only some of them are applicable to Direct SPIT. These techniques are introduced in this section.

A powerful technique against e-mail spam is content filtering. Unfortunately, this is not applicable against SPIT.

Content filters have a lot of time to check the mail before it is sent to the recipient. Unfortunately, the content of a call is not available in advance. However, SPIT has to be detected

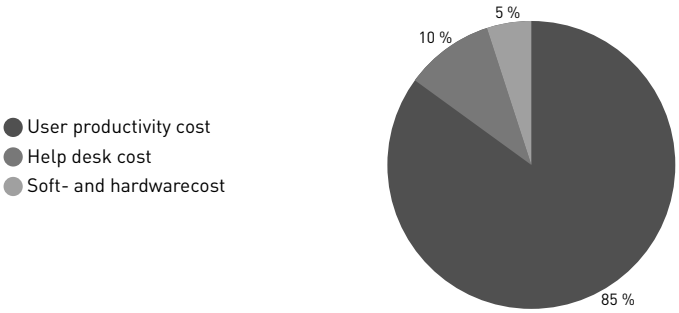


Fig. 5. Percentage of economic damage caused by e-mail spam [4].

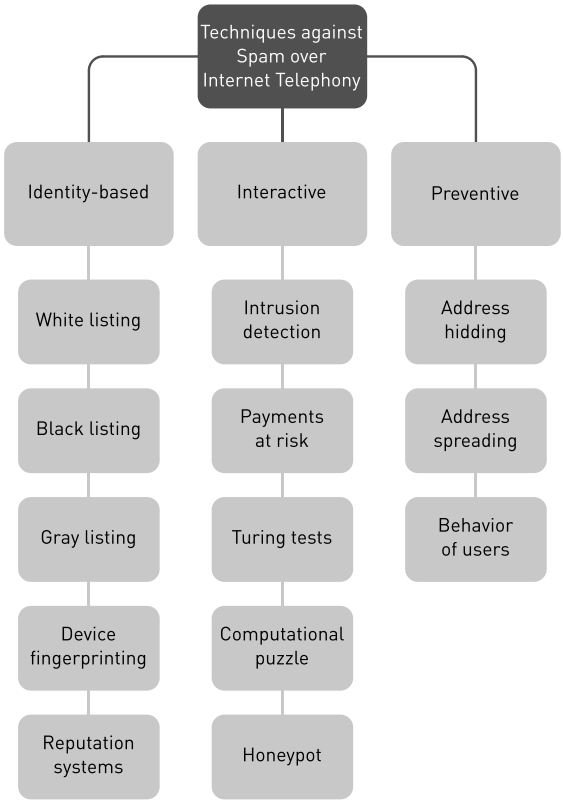


Fig. 6. Categories of techniques against SPIT.

before the phone is ringing, because the callee is actually annoyed when that happens.

So, it is important to look at the capabilities of the available user equipment. A usual phone is not able to process large amounts of data or to store much information. Some techniques against SPIT are depicted in Figure 6. These are discussed in more detail in the following.

### A. Identity-based Techniques

Identity-based techniques attempt to avoid SPIT by the analysis of static information. They are able to fend spam utilizing only few resources in hardware and processing time. These techniques are the following:

- White listing: A white list is a list, which contains a collection of addresses of trusted users. Only calls from addresses that are present in this list are allowed to connect to the callee. The decision is made by comparing the address of the sender to the entries in this list.
  An attacker needs good knowledge about the social connections of his victim to bypass white listing. It is a very strong protection against unwanted communications, but on the opposite side is it too strong. All regular people cannot contact a protected user as long as they are not listed.
- Black listing: A black list is the technique opposite to white listing. All calls from addresses on the list are rejected.
  It is rather easy to bypass black listing. An attacker only has to change the source of his message, after he realizes that he is blocked. A service provider has to be very careful before he black lists a participant, because he must avoid listing a legitimate one.
- Gray listing [13]: The main disadvantage of black- and white listing is that the caller has to be known in advance. In this case, a gray list is applicable. Here, an initial call attempt is generally rejected. If the caller starts a second call attempt in a given time, his call gets connected to the callee.
  This technique is rather simple to bypass for an attacker by calling a second time if the first time misses. However, it is annoying for the caller to be rejected after an initial call attempt if he is not known in advance (e.g., a bank clerk).
- Device fingerprinting [14]: This technique analyzes the structure of the message or user equipment behavior to decide whether to accept the call attempt or not. Therefore, knowledge about behavior and message structure of well-known user equipment has to be available. The call attempt gets connected if its structure or the calling user equipment's behavior is successfully identified.
  This technique uses the assumption that spammers use their own self made soft phones, which are able to distribute more SPIT. An attacker who uses a common soft phone cannot be rejected by this technique. However, a spammer only has to imitate a known soft phone if he makes his own one.
- Reputation systems [15]: Each user gets an individual rating derived from user-based evaluations. Users with good ratings are allowed to call and users with bad ratings are blocked.
  This technique originates from e-commerce. Therefore, it suffers the same problems with reputation mafias. These try to increase (ballot stuffing) or decrease (bad mouthing) the reputation score [16]. This could be done by a botnet, for example.

The techniques belonging to this group are the easiest to implement in user equipment. Only device fingerprinting needs too much up-to-date information to work properly. So, it cannot be used to fend Direct SPIT directly.

TABLE I
CPT EXAMPLE FOR REQUEST INTENSITY [17].

| | INVITE | REGISTER | ACK | CANCEL | BYE |
|---|---|---|---|---|---|
| Regular attack | 30 % | 10 % | 30 % | 10 % | 10 % |
| Scan attack | 40 % | 5 % | 40 % | 10 % | 5 % |
| SPIT | 40 % | 0 % | 40 % | 0 % | 20 % |
| Denial of service | 90 % | 10 % | 0 % | 0 % | 0 % |
| Password cracking | 10 % | 40 % | 40 % | 0 % | 0 % |
| Firewall traversion | 40 % | 0 % | 40 % | 0 % | 20 % |

### B. Interactive Techniques

Interactive techniques are designed to increase the cost for the distribution of SPIT. Their purpose is to raise that cost as much as possible to make SPIT too expensive for the sender. A description of these techniques follows:

- Intrusion detection [17]: This technique analyses the network traffic and compares it to usual traffic. It is designed for multiple network attack, but can also be used against SPIT. Intrusion detection cancels the call attempt if the traffic looks similar to an attack.
  The decision whether a flow is an attack or not is made with a conditional probability table (CPT). This CPT contains expected information about request intensity, error response intensity, number of destinations, etc. Many transmitted INVITE requests may be a probable indicator for SPIT, as depicted in Table I. Unfortunately, there is no knowledge about SPIT attacks and their behavior. Therefore, the CPT of the intrusion detection system can only be filled with information based on assumptions.
- Payments at risk [18]: The caller has to send a small amount of money to the callee. He gets his money back if the callee declares that the call was desirable. This technique leads to a direct increase of costs.
  Unfortunately, this technique generates a huge amount of financial transactions. Furthermore, it is problematic if the SPIT is initiated by a soft phone, which is remote-controlled by a bot.
- Turing tests [19]: A Turing test has the purpose to differentiate between human and machine. Therefore, a sound file is played to the caller. The sound file contains a short voice message, maybe in a dialect or containing background noise. Here, the sound file is relayed to a human, who solves it. The caller gets connected if he repeats this message correctly.
  This technique can be bypassed by a relay attack. Therefore, the sound file is relayed to a human, who solves it. This can be done by a call center, for example.
- Computational puzzle [15]: A computational puzzle is designed to increase the required hardware resources and calling time of the spammer. The calling user equipment has to calculate a task, which is very hard to solve. The caller gets connected after the correct result is transmitted.
  However, a computational puzzle is not able to prevent a victim from SPIT. The soft phone of a spammer is able to solve the task as well. Therefore, the result of a computational puzzle is only an increase of processing time at the caller.
- Honeypot [15]: Honeypots try to bind resources of spammers as long as possible. An incoming call is processed very slowly to bind the spammer's user equipment.
  A honeypot can be used as a SPIT monitoring system as well. It records all information about incoming SPIT and, therefore, allows an analysis of it.

Turing tests and computational puzzles are the weakest of these techniques. A spammer still gets connected even if a computational puzzle is in use. A Turing test does not represent a prevention for SPIT that is sent from a call centre. However, this group of techniques needs too many resources to run on user equipment and hence to be implemented within.

### C. Preventive Techniques

Preventive techniques have the purpose to avoid SPIT before it occurs. The main goal is to keep spammers from gathering addresses.

Unfortunately, these techniques are not designed to work on user equipments. They concern the behavior of the user. This cannot be done by any equipment.

## IV. CALLER PRE-VALIDATION MECHANISM

The callee's user equipment has to decide about the confidentiality of an incoming call. Therefore, a pre-validation mechanism is presented in this section.

### A. Requirements

The pre-validation mechanism has to fulfill some requirements in order to be useful. Furthermore, it has to match some additional requirements, because it will be used in our research project Next Generation Telco Factory (NextFactor). They have the objective to enable a better integration as well as higher security. These requirements are the following:

- Standard compliant: The concept should work without any changes or preconditions to the equipment of the caller and service provider. A mechanism without this constraint would not work while the spammer uses a non-compliant soft phone or service provider. Furthermore, all requests should be used in their specified meaning.
- Open source software: The NextFactor research project uses open source software from its very beginning. This demands to use future open source components to fulfill the license requirements of the ones, currently in use. These yet used software is under the terms of the GNU General Public License version 2 (GPLv2) [20]. Therefore, the future software must also be compliant to this license.

These requirements should improve the quality of the resulting mechanism. The standard conformity is important, to ensure success.

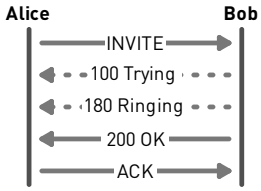


Fig. 7. Progression of a usual incoming call.

### B. Analysis

Even with the lot of techniques presented in Section III, there is no feasible protection against Direct SPIT possible. The most techniques are designed to work in the proxies of the provider's network. Unfortunately, these proxies are bypassed by Direct SPIT. A technique is needed that is able to prevent Direct SPIT with the capabilities of usual user equipments.

Three problems could be identified:

- Lack of information in the user equipment: Most techniques require very up-to-date information to work properly. A listing technique cannot act against a spammer before the list does not know that he is a spammer. This information is much easier to distribute between proxies of the provider's network.
- Lack of processing power: For example, an intrusion detection mechanism requires too much processing power to run efficiently on a user equipment.
- Lack of time: The user equipment starts to ring immediately, after an initial INVITE request arrives, as shown in Figure 7. This is expressed with the optional 180 Ringing response sent back after the arriving INVITE request (and the also optional 100 Trying response). Therefore, there is no time left to do any validation. Nevertheless, it is still too late at the moment the phone starts ringing, because this disturbs the callee.

Let assume, that the callee's user equipment has enough time. It needs at least a little information about the caller, to verify his existence. There is only one INVITE request available at that time. Anyway, there is useful information about the caller in the SIP URI of the request (e.g., sip:alice@example.com):

- The user name (i.e., "alice").
- The name or IP address of the provider being used (i.e., "example.com").

It is important to keep the 180 Ringing response until validation succeeds. Therefore, the user equipment has time to validate the caller.

### C. Concept

The user equipment has only a little information about the caller, as explained above. Now it has to validate its correctness. However, there is still no guarantee that SPIT will not occur. It can only be assured that the caller is registered. This is important, because it is very likely that spammers use Direct SPIT, since they do not want to use valid accounts. The named provider is able to admonish a user, after he sends SPIT if he is a registered user of the provider. There are two steps to perform after separating the 100 Trying and 180 Ringing response, as visible in Figure 8:

- Check the existence of the caller at the provider.
- Check the existence of the caller's user equipment.

The call attempt can be rejected if this information is not correct, because the caller is not trustable. The call establishment can proceed if the existence of the calling user is confirmed.

Therefore, a way to validate the existence of the user at the named provider is needed. The SIP Specific Event Notification [19] is helpful to do this. It provides several event packages for different scenarios. The following event package-based mechanism and event packages are applicable to the Direct SPIT:

- Presence event package [21]: This package allows getting information about the presence state of a user. A presence state is the willingness and ability of a user to communicate. It is widely common in instant messaging. The subscriber is notified if the requested user changes his presence state (e.g., from "present" to "away").
- INVITE-initiated dialog event package [22]: This package has the purpose to inform a subscriber if the requested user changes his dialog state. It is usable with all SIP messages that result in a dialog (e.g., INVITE, SUBSCRIBE). The requesting user gets a NOTIFIY request if such a dialog changes his state (e.g., "terminate").
- Dialog Event foR Identity VErification (DERIVE) [23]: This mechanism makes use of the INVITE-initiated dialog event package to verify that the current caller is in the correct state (i.e.,"Proceeding"). Besides, the state is verified that the caller is a known member of the alleged service provider. The outcome of the use of DERIVE can result in three cases.
  The call is verified if the SUBSRIBE request is answered with a 200 OK response. The correct state of the caller is confirmed in the following NOTIFY request.
  The call cannot be verified if the service provider of the caller does not support the Dialog Event Package. A 489 Bad Event response returns to show this. Nevertheless, the call attempt is accepted, because it is not mandatory to support this event package.
  The call attempt is suspicious if the answer indicates that

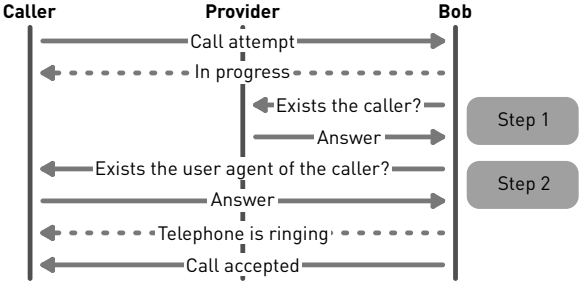


Fig. 8. Conceptual changes in a call attempt.

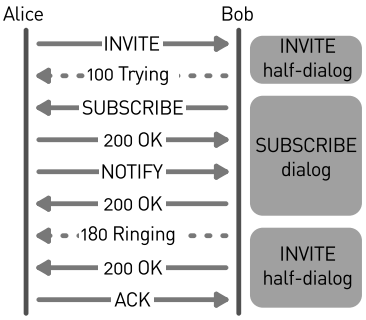


Fig. 9. Overview of DERIVE operation [23].

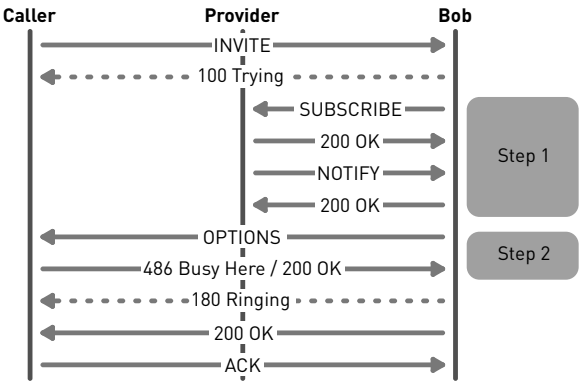


Fig. 10. Released changes in a call attempt.

the caller is not currently in the proceeding state. Therefore, the call attempt is rejected with a 434 Suspicious Call response.

The next validation step can be started if the user's existence at the provider has been validated. It is desired to validate the user equipment of the caller. This validation is important, because otherwise probable spammers are able to send messages with incorrect IP addresses.

Spammers are not able to start a bidirectional communication with an incorrect IP address, maybe it is only desired to disturb the callee. Therefore, spammers only have to send one INVITE request, because most user equipments starts to ring immediately.

A request can be sent to the calling equipment directly to validate the user equipment. The following three requests are the most suitable:

- MESSAGE: This request transmits a text message to its destination. The use of this request has some disadvantages. A second validation could be started if the recipient wants to validate the request as well. This leads to a loop if he uses the same validation. Additionally, it is possible to annoy a uninvolved third user if the caller sends an assigned IP address.
- INVITE: The purpose of the INVITE request is to establish a phone call. It has the same disadvantages as the MESSAGE request. Additionally, it is possible to connect the callee to a premium rate service with high rates, for example. However, the callee has to act by himself to become a victim of such an attack.
- OPTIONS: The OPTIONS request is normally used to determine the capabilities of user equipment. A communication is not established, so the disadvantages of the above requests do not apply here. The receiving user equipment does not act recognizably for its user and, therefore, does not annoy him.

### D. Proof of Concept

The presented concept was implemented with Android 1.5 [24] and the VoIP client sipdroid 1.0.8 [25].

The Presence Event Package is used to validate the existence of the user at the provider, as depicted in Figure 10. This decision is made because the Dialog Event Package requests some information, which has nothing to do with the existence of the user. Using the presence state fits better to this task. It is a more expressive information about the "current" existence.

The validation of the user equipment is done by sending the OPTIONS request, because this is the only request without the disadvantage of possible annoyances. However, the contact header field of the NOTIFY request is validated before the OPTIONS request is sent. The OPTIONS request is not sent if it contains the temporary SIP URI of the caller. The existence of the user equipment is validated by comparing its address to the sender's address of the INVITE request, instead of sending the OPTIONS request. Therefore, the transmission time for this request is saved.

### E. Restrictions

The presented mechanism is not able to work in every possible network configuration. Most of all, a presence server is required, which is not mandatory for a standard SIP configuration. However, future VoIP networks most likely include a presence server, as the IP Multimedia Subsystem (IMS) [26] concept becomes more popular. A 434 Suspicious Call response [23] could be sent out if the caller has no presence server available. Therefore, he gets adequate information why his call attempt is rejected.

Another scenario where no pre-validation is applicable is an anonymous caller. Anonymous calls are still known from public switched telephony. These calls are often mistrusted, because the callee expects that the caller has something to hide. In the sense of this behavior is it most fitting to sent a 433 Anonymity Disallowed response [27] to the caller. A caller who really wants to call the callee can see the reason of the rejection and call again without anonymity.

## V. Attacking Scenario

The proposed caller validation has a main vulnerability. Let assume that the attacker has at least one valid account (i.e., sip:dummy@example.com) in the provider's network of the target, as depicted in Figure 11. The spammer calls Bob by his temporary SIP URI from a second unregistered account (i.e., sip:spammer@192.0.2.1). Then the INVITE request contains the information that it is allegedly sent from the registered

account. The provider confirms this request and sends a NOTIFY request, due to the fact that this account is registered.

This NOTIFY request must contain the header field "contact". It is not specified, which address has to be written in there. Hence, two possible scenarios can occur:

- The contact address in this message contains the temporary SIP URI of the registered account. Therefore, the user equipment rejects the call attempt, because it differs from the one in the INVITE request.
- The contact address does not contain the temporary SIP URI. Instead, there is maybe the address of the presence server. Now, the OPTIONS request is sent to the permanent SIP URI. However, this message is transmitted to the registered account of the spammer that really exists. So, the validation succeeds, too.

The proposed caller validation mechanism offers no protection in the second scenario. However, this attack works only if the presence server does not sent the temporary SIP URI of the spoofed account.

## VI. Performance Analysis

It is obvious that the proposed mechanism requires more time to process than a normal call attempt. This section contains an analysis about this durational increase and its amount.

### A. System Under Test

To determine the difference in processing time, a system with a 1.66 GHz dual core processor, 2 GB memory and a 6 Mbps internet connection was used. The SIP proxy of the provider was located in Denver (USA) Caller and callee were located in Darmstadt (Germany). The distance between Denver and Darmstadt is about 8,000 km, which results in 200 ms round-trip time with 17 hops. The caller pre-validation prototype was launched inside the Android Emulator.

### B. Key Performance Indicator

One key performance indicator was defined to ensure stable and comparable measurement results. The start trigger of the time measurement is at the arrival of the INVITE request, as depicted in Figure 12. The stop trigger is at the sending of the 180 Ringing response.

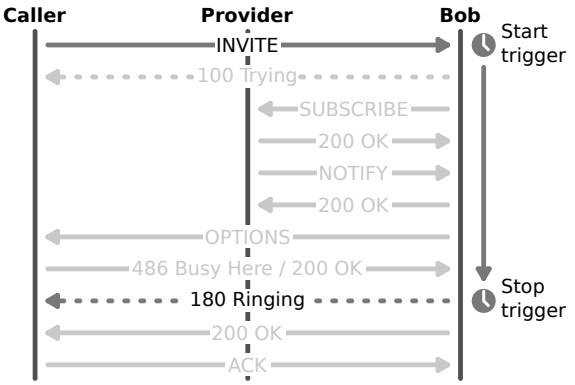


Fig. 12. Start and stop trigger of the service processing time.

The measurement takes place at the user equipment. This should reduce the distortion of the first and last message transmission to the caller, which does not depend on the pre-validation mechanism. The rest of the session establishing process was not measured, because it is the same as without caller pre-validation. The test sequence was repeated a hundred times.

### C. Test Results

The regular sipdroid needs an average of 2.821 s to produce an answer, the prototype sends the answer after 5.240 s. A five-number summary of the results is listed in Table II and depicted in the box plot in Figure 13. It is obvious that the maximum results are outliers, because they are that much away from the box. Both clients show a similar behavior in processing and answering. This leads to the assumption that the mechanism has no negative influences on stability.

To confirm this assumption, the 95 % confidence interval was calculated. Itis shown in Table III and Figure 14. Both expected values are located within the same range. The main difference is that the caller pre-validation prototype requires about 2.5 s longer to process an answer. These 2.5 s contains a round-trip delay of 0.2 s per message to Denver and hence

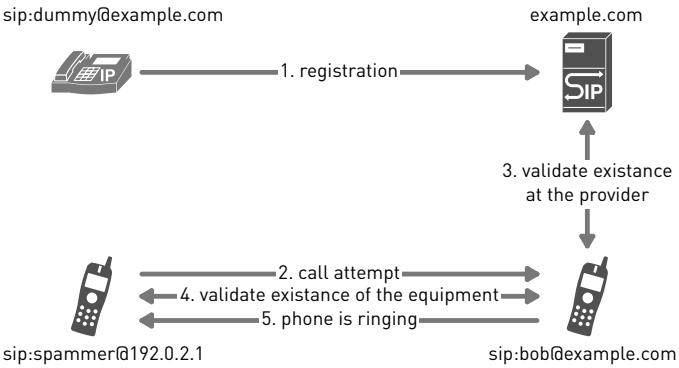


Fig. 11. Successful attacking scenario.

TABLE II
Five-number summary of the test results.

| | Minimum | 1. quartil | Median | 3. quartil | Maximum |
|---|---|---|---|---|---|
| Sipdroid | 2,405 s | 2,531 s | 2,837 s | 3,000 s | 3,538 s |
| Prototype | 4,759 s | 5,016 s | 5,186 s | 5,417 s | 6,003 s |

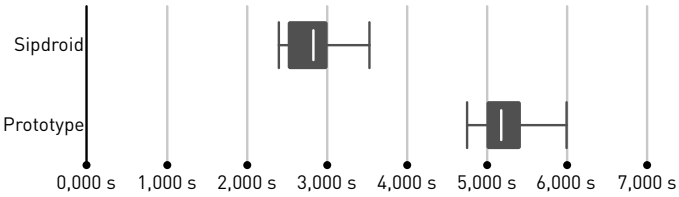


Fig. 13. Box plot.

TABLE III
VALUES OF THE 95 % CONFIDENCE INTERVAL.

| | Lower | Average | Upper |
|---|---|---|---|
| Sipdroid | 2,764 s | 2,821 s | 2,879 s |
| Prototype | 5,181 s | 5,240 s | 5,298 s |

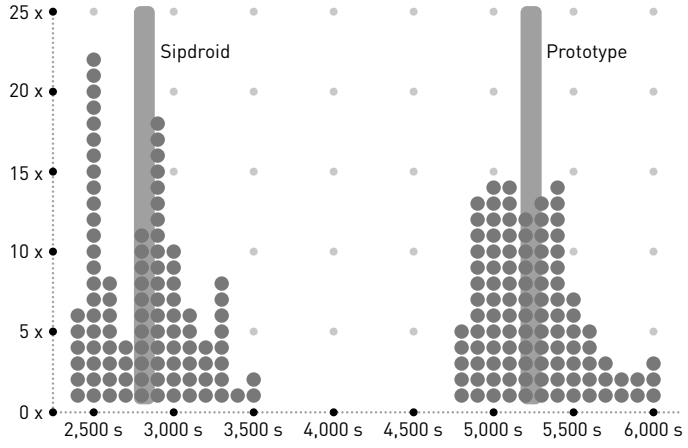


Fig. 14. 95 % confidence interval.

is smaller if a local provider is used.

These additional 2.5 s are only relevant to the caller. A callee never notices this time span, because his user equipment does not ring until it is done. Furthermore, this is an additional time needed for spammers. They can send less spam per hour if a huge number of their victims use this mechanism. So, this approach could be treated as an interactive technique to make spamming unprofitable.

It has to be mentioned that these results are based on a prototype that still needs some optimization. Its only purpose was to provide a proof of concept.

## VII. Conclusion and Future Work

The defense against Direct SPIT is relevant for a large number of internet users who want to communicate over the internet via VoIP. The caller pre-validation mechanism introduced in this article is able to fend Direct SPIT sent from unregistered users. This is important because it is probable that spammers use Direct SPIT from unregistered accounts in order to be undetectable. However, the presented mechanism is only able to validate the correctness of the given user information. Furthermore, even a registered user is able to send SPIT. There is no guarantee that SPIT will not occur while using this mechanism. However, the caller's provider is capable to take measures against such users.

The prototype is currently in an alpha phase. It has to be implemented more efficiently, because a delay of 2.5 s is still a lot of time. This delay is indeed only observable for a caller – but this can be a legitimate caller, too. Therefore, the transmission of the SUBSRIBE and OPTIONS requests have to be made in parallel. The goal is to drop the delay to 50 % of the achieved value. The comparison of the temporary SIP URI in the NOTIFY and INVITE request can be performed after all responses have arrived.

Furthermore, an analysis has to be conducted regarding opportunities to fix the weakness in the attacking scenario described in Section V. If it is possible to fix the vulnerability, this would be included in the concept as well as in the prototype.

Additionally, the blocked callers could be added to a gray- or black list to save some time and processing power for an additional call attempt.

The prototype will be included into other VoIP clients as soon as it will be running robustly and more efficiently. Therefore, an implementation for a research project of the Department of Computer Science will be made.

## VIII. Acknowledgements

We would like to thank Rachid El Khayari from the Fraunhofer Institute for Secure Information Technology for his wise support, which makes this work possible. We would also like to thank our valuable reviewers especially Torsten Wiens for his extensive and high quality comments.

## References

[1] J. Müller and M. Massoth, "Defense against direct spam over internet telephony by caller pre-validation," in *Proceedings, The Sixth Advanced International Conference on Telecommunications (AICT 2010), 9-15 May 2010, Barcelona, Spain*, J. E. Guerrero, Ed. Los Alamitos, CA, USA: IEEE Computer Society, 2010, pp. 172–177.

[2] *The IT Security Situation in Germany in 2009*, Federal Office for Information Security, Bonn, Germany, Jan. 2009.

[3] *MessageLabs Intelligence August 2010*, MessageLabs, New York, NY, USA, Aug. 2010.

[4] R. Jennings, "Cost of spam is flattening," Ferris Research Blog, http://www.ferris.com/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions/ 20.01.2011.

[5] *The Carbon Footprint of Email Spam Report*, McAfee, Santa Clara, CA, USA, 2009.

[6] M. Machowinski and D. Myers, "Trend toward hosted and business voip services seen across three new reports," Infonetics Research Press Release, Apr. 2010.

[7] Federal Association for Information Technology, Telecommunications and New Media, "Erstmals mehr als 10 millionen nutzer von internet-telefonie," Press statement, Apr. 2010.

[8] E. Potter, "Number of mobile voip users will approach 300 million by 2013," In-Stat Press Release, Mar. 2010.

[9] R. El Khayari, N. Kuntze, and A. U. Schmidt, "Spam over internet telephony and how to deal with it," in *Proceedings of the ISSA 2008 Innovative Minds Conference, 7 - 9 July 2008, School of Tourism & Hospitality*, H. S. Venter, M. M. Eloff, J. H. P. Eloff, and L. Labuschagne, Eds. Johannesburg, South Africa: University of Johannesburg, 2008.

[10] *Why Am I Getting All This Spam?*, Center for Democracy & Technology, Washington, DC, USA, Mar. 2003.

[11] T. Eggendorfer, *No Spam! Wie Spam gar nicht erst entsteht*, 1st ed. Frankfurt am Main, Germany: Software & Support, 2005.

[12] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "Sip: Session initiation protocol," RFC 3261, IETF, Jun. 2002.

[13] E. Harris, "The next step in the spam control war: Greylisting," http://projects.puremagic.com/greylisting/whitepaper.html 20.01.2011.

[14] H. Yan, K. Sripanidkulchai, H. Zhang, Z.-Y. Shae, and D. Saha, "Incorporating active fingerprinting into spit prevention systems," in *3rd Annual VoIP Security Workshop, Berlin, Germany*. New York, NY, USA: ACM, 2006.

[15] J. Rosenberg and C. Jennings, "The session initiation protocol (sip) and spam," RFC 5039, IETF, Jan. 2008.

[16] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *The 2nd ACM Conference on Electronic Commerce (EC 2000), Minneapolis, MN, USA – October 17 - 20, 2000*, A. Jhingran, J. K. MacKie-Mason, and D. Tygar, Eds. New York, NY, USA: ACM, 2000, pp. 150–157.

[17] M. El Baker Nassar, R. State, and O. Festor, "Intrusion detection mechanisms for voip applications," in *3rd Annual VoIP Security Workshop, Berlin, Germany*. New York, NY, USA: ACM, 2006.

[18] M. Abadi, A. Birrell, M. Burrows, F. Dabek, and T. Wobber, "Bankable postage for network services," in *Advances in Computing Science – ASIAN 2003: Progamming Languages and Distributed Computation, 8th Asian Computing Science Conference Mumbai, India, December 10-12, 2003, Proceedings*, ser. Lecture Notes in Computer Science, V. A. Saraswat, Ed., vol. 2896. Berlin / Heidelberg, Germany: Springer, 2003, pp. 72–90.

[19] H. Tschofenig, E. Leppanen, S. Niccolini, and M. Arumaithurai, "Completely automated public turing test to tell computers and humans apart (captcha) based robot challenges for sip," Internet-Draft, IETF, Feb. 2008, expired: 28.08.2008.

[20] *GNU General Public License Version 2*, Free Software Foundation, Boston, MA, USA, Jun. 1991.

[21] J. Rosenberg, "A presence event package for the session initiation protocol (sip)," RFC 3856, IETF, Aug. 2004.

[22] J. Rosenberg and H. Schulzrinne, "An invite-initiated dialog event package for the session initiation protocol (sip)," RFC 4235, IETF, Nov. 2005.

[23] J. Kuthan, D. Sisalem, R. Coeffic, and V. Pascual, "Dialog event for identity verification," Internet-Draft, IETF, Oct. 2008, expired: 28.04.2009.

[24] Open Handset Alliance, "Android.com," http://www.android.com/ 20.01.2011.

[25] P. Merle, "sipdroid - project hosting on sip/voip client for android," http://www.sipdroid.org/ 20.01.2011.

[26] Technical Specification Group Services and System Aspects, "Ip multimedia subsystem (ims); stage 2 (release 10)," 3rd Generation Partnership Project, Technical Specification TS 23.228 V10.3.1, Jan. 2011.

[27] J. Rosenberg, "Rejecting anonymous requests in the session initiation protocol (sip)," RFC 5079, IETF, Dec. 2007.