

Spam over Internet Telephony with SPITFILE

Jan RŮŽIČKA, Miroslav VOŽNÁK, Filip ŘEZÁČ • <janru@cesnet.cz, miroslav.voznak@vsb.cz, filip.rezac@vsbcz>
 CESNET, z.s.p.o. • Zikova 4 • 160 00 Prague • Czech Republic

Abstract

One of the most extended attacks in the Internet environment is Spam. It is estimated that Spam takes **80 - 90% of total attacks** on the Internet. Security experts predict that Spam over Internet Telephony (SPIT) will be a major threat in the future. The level of annoying factor is even greater than classical Spam.

On an average we receive 5 Spam emails per day and we delete them and most of us have to take this as a daily routine. Now instead of unwanted emails we can imagine a machine generating many calls and replaying a message. It is really inconvenient thought.

An experimental SPIT attack has been developed as an application at CESNET. The software was given a name **SPITFILE** and has been written in Python and based on the famous call generator Sipp. The presented paper deals with the SPITFILE as an example of SPIT attack and of course, how to defend against these attacks.

Aim

We want to point out that **SPIT is not a mere theoretical threat** anymore but a real and a very dangerous risk in IP telephony.

This paper is intended to serve as an example how easily can attacks of SPIT type be implemented in Voice over IP networks. The paper also describes possible defences against such a type of attack.

Method

To simulate a **SPIT** attack, we have used SIP and RTP packets generator called Sipp. This application is open-source and works under both Linux and Windows distributions. Sipp works with preconfigured diagrams in .xml format and transmission properties are set using parameters in the command line. Our application called **SPITFILE** implements a graphic interface for Sipp and works with ready-made .xml diagrams. Thus, the simulation of a SPIT attack is much simpler. SPITFILE was programmed in **Python** using wxPython GUI. Its control is very intuitive – the requested values are submitted into relevant fields and to the SPIT attack is launched with SEND button. SPITFILE is available only for Linux distribution now but the source code for Windows should be completed soon too. For a proper operation of the SPITFILE application it is first necessary to install the following packages: Python≥v2.6, Sipp≥v2.1, Python-wxgtk≥v2.6. Our application can generate two types of attacks.

Direct – It generates SPIT on IP phone directly in the local network without using the VoIP PBX (some IP phones can refuse a direct calls that avoid SIP Proxy, the Proxy mode is more suitable for such cases).

Proxy – It generates SPIT via VoIP PBX (SIP Proxy) and the attack thereupon can run against anything that is available behind the Proxy theoretically involving not only IP phones but also ordinary phones and overall telephone world. It is necessary to obtain a user account because a successful registration at SIP Registrar is required before the calls via SIP Proxy can be performed.

Results

Before SPITFILE can be opened, preconfigured .xml diagrams (direct.xml and proxy.xml) should be imported into /etc/ directory. Afterwards we can launch SPITFILE and choose one of two the above mentioned attacks that we want to carry out.

To run SPITFILE, just type the following command into the terminal: python <location of the **SPITFILE.py** file>. In **Direct mode**, only target phone IP address, number of calls, time between calls and finally an advertisement message which will be replayed need to be defined. The called phone rings after the attack has been sent and a **pre-recorded voice message will be replayed** after the incoming call is answered.

SPITFILE has been tested with HW Grandstream IP phones (GXP 2000, 3000) and with SW IP phones (Sjphone and X-Lite). The **Proxy mode** has additional fields such as the required account which is consequently used for registration, i.e. SIP number, username and password. The other fields are the same as in the case of previous Direct type. We have tested Asterisk PBX and Siemens hipath4000 PBX.



Direct

Proxy

Sipp started by SPITFILE

Now, how can one defend against such a type of attacks? There are several methods which can be implemented to protect the VoIP equipments from SPIT attacks.

Buddylist/ Whitelist - Every subscriber has a list of subscribers. Those who are not on the list cannot initiate a call. The problem arises when the subscribers that are not on the list are regular callers and we would like to speak to them. To allow the calls from subscribers who are not on the whitelist is helpful to access a 'web of trust.' Each subscriber grants his trust to several other subscribers.

Blacklist - This is a reversed whitelist.

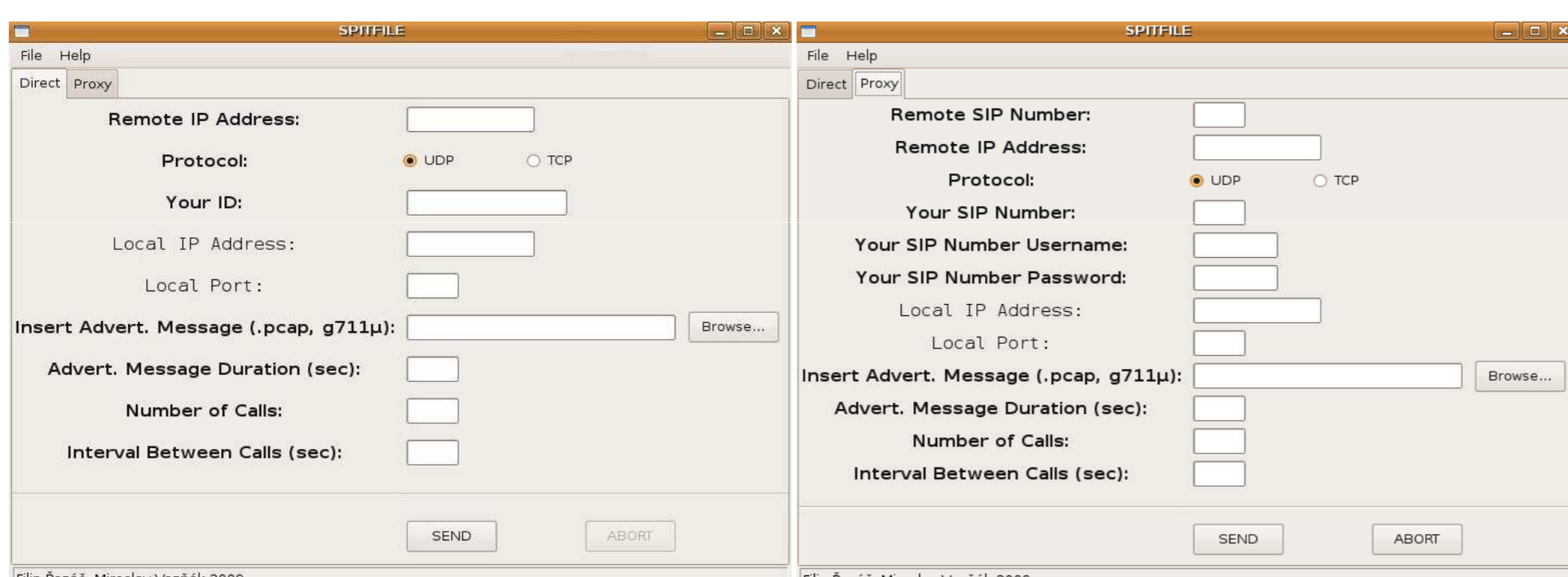
Statistical blacklist – Telephone providers carry out different analyses and apply different statistical methods to create a spammer list.

Voice menu interaction – Before the caller is actually put through to the called subscriber, the caller is directed to the voice menu where he is asked to enter a numeric code (e.g. 123*) to be able to get through to the caller. This protection is effective against caller bots (relatively until the bots take up using a speech recognition).

Greylist – This is a modified blacklist (whitelist) under which the phone returns the engaged line tone to the caller who is making the call for the first time. This time, the phone does not actually ring on the called subscriber. If the caller attempts to make the connection again the call is connected. It increases a likelihood that the caller is a human person and not a SPIT bot.

Conclusion

The paper dealt with SPIT attacks and methods to initiate such attacks. For this purpose, we developed a SPITFILE application. Some of the above described security measures or combination thereof should be implemented in every IP ready PBX. This should enhance the protection against SPIT attacks. However, effective SPIT attack methods can be developed very fast and further intensive research is needed to guarantee the security of VoIP systems. Fortunately, most of telephone calls are charged which functions as a brake but we cannot not rely on it. SPIT is a threat hanging like the sword of Damocles over the telephony world. This paper proves that it is not a mere speculation but a reality.



Direct

Proxy

SPITFILE application example