



Eyeball AntiSPIT Technology

www.eyeball.com

Copyright 2005

Introduction

Voice-over-IP (VoIP) is getting widespread adoption both from business and residential customers. VoIP uses standard and open protocols such as Session Initiation Protocol (SIP) or Real-Time Protocol (RTP) for voice and video call establishment and data transfer. Using common computer technology and open standards for VoIP makes users vulnerable for the various security problems already occurring in common Internet applications. These vulnerabilities include:

- Bulk and unsolicited calls for telemarketing, recorded advertisements and other commercial purposes from anywhere in the world, at any time,
- Harassment and abuse such as repeated automated calls,
- Malicious service attacks leading to service disruptions (such as massive automated calling from multiple machines), and
- Exposure to unacceptable content such as illicit content or offensive language from strangers (a big issue specifically with children and women).

We use the term VoIP “spam over Internet telephony” or just “SPIT” to refer to the problems described above and the term “spitter” describes VoIP users sending SPIT. If VoIP SPIT cannot be prevented it may victimize any user including traditional telephony system users (i.e. PSTN and mobile phone users). The mere volume of potential SPIT calls using VoIP technology, where making a million calls becomes as simple as making a single call, may render phone systems unusable.

Over two-thirds of the emails sent through the Internet currently represent spam emails. However, if proper measures are not taken against VoIP SPIT, it will be a worse problem than the current email problem as VoIP calls require real-time attention from callees and SPIT may make the traditional PSTN system unusable (due to the volume of SPIT calls sent from VoIP systems).

Consequently, the mechanism employed by any AntiSPIT solution must not employ fixed limits for single sources, but be usable in a way that complying users will not notice the AntiSPIT mechanisms are in effect.

Requirements for SPIT-prevention

In a simplified view, a communication system such as PSTN or a VoIP system consists of two main components, the server system maintained by the service providers and the end-points used by customers (residential or business). An end-point may be a hardware phone, a hardware videophone, a TV phone, or a software phone or messenger. In order for VoIP and video telephony to be successful as a mainstream communication system, it should meet the following requirements with respect to SPIT protection:

1. The server system should be able to forward “good” calls and block SPIT, while flagging suspicious calls before they are forwarded; and

2. The end-points should provide robust, simple and flexible means to protect end users from SPIT calls.

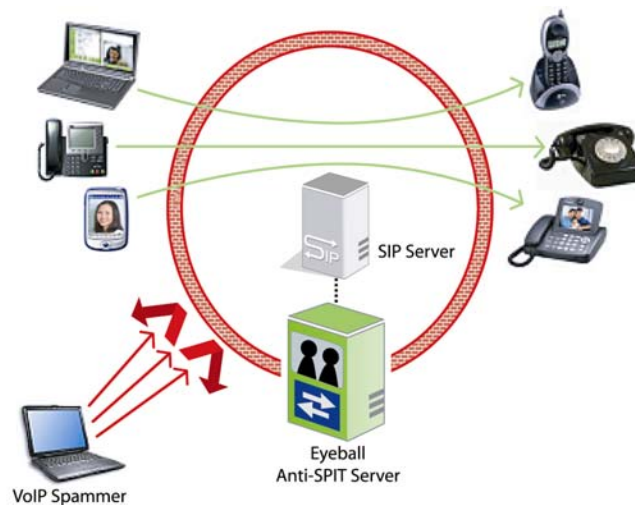
The server system has the following desired features:

- Dynamic monitoring and control of the service provided and the SPIT prevention mechanisms;
- Preventing bulk unsolicited calling;
- Blocking calls from non-complying callers.
- Prevent “false positives”, i.e., avoiding complying users being blocked
- Providing minimal additional administration effort

The end-points have the following desired features:

- Valid calls from other users will not be blocked;
- Callees must have an easy and simple way to avoid SPIT calls and bad content (such as using green, yellow and red color coding);
- Users may set call filters based on validated user IDs, geographic location of callers, time of day etc.
- User interaction to avoid SPIT is minimal
- Parental control mechanisms are available to restrict call sources, destinations, total calling time, time-of-day, and call content, in particular for video calls.

The patent-pending Eyeball AntiSPIT technology supports those previously outlined requirements, providing a safe environment for subscribers while keeping the overall administrative effort for service providers low.



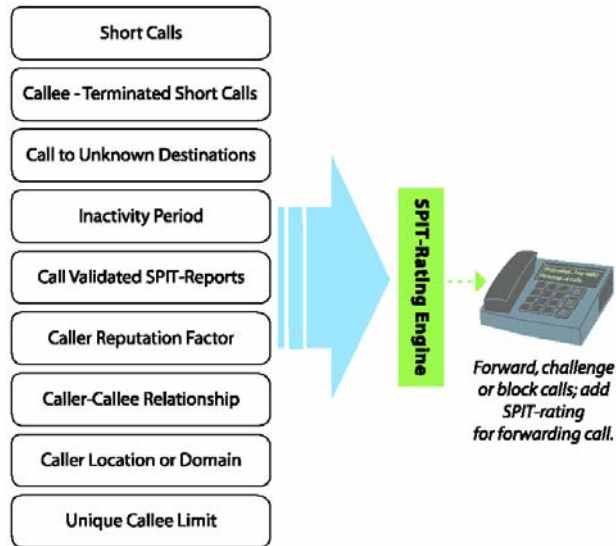
Eyeball's AntiSPIT Technology secures existing SIP servers to provide a SPIT-free environment.

Eyeball AntiSPIT Technology

The patent-pending Eyeball AntiSPIT technology is fully compliant with SIP (RFC3261) based VoIP environments. On the server-side, it is integrated into the latest version of the Eyeball Video Communications Server and also available in the stand-alone Eyeball

AntiSPIT Server, which interoperates with existing SIP server installations. Additional client protection is provided in the latest version of the Eyeball SDK.

Dynamic AntiSPIT Engine



Overview: Eyeball AntiSPIT Engine Input and Features

For bulk calling to be attractive to potential spitters, the spitters need to make a large number of calls to a large number of callees within a short period of time. This is restricted by the Eyeball AntiSPIT technology by limiting the number of calls output and calls received for a single user (e.g., based on routable identity such as SIP URI) or a hardware device (e.g., based on IP address).

The dynamic AntiSPIT engine as the foundation of the Eyeball AntiSPIT technology monitors call patterns, SPIT events and other relevant data to control calling rate limits of callers. The dynamic approach limits only callers showing suspicious behavior, thus ensures legitimate callers will not be affected while SPIT is effectively prevented.

- Dynamic Calling Rate Limit

The AntiSPIT engine employs a calling rate that is dynamically adjusted such that abnormal calling behavior leads to a reduction of the ability to carry out SPIT calls while not interfering with legitimate calls. The algorithm combines various criteria related to SPIT, including the caller-callee relationship, and combines this information into a single value used as dynamic calling rate limit for each caller. Once the calling rate limit is exceeded, further calls can be blocked, challenged or forwarded with a tag to the callee.

- Unique Callee Limit

Mass calling also requires a large number of callees. The unique callee limit can be employed to restrict the number of unique callees for callers or caller groups.

The AntiSPIT engine different computes dynamic calling rate limit and unique callee limit based on various factors such as call patterns, caller location, and caller-callee relationship. The Eyeball AntiSPIT engine combines those factors to compute a single value, which defines the actual dynamic calling rate limit of a caller. Initially, callers are not limited in their capability to make calls. Only incidents related to SPIT calls lead to a reduction of the calling rate. Using this mechanism, only non-complying callers are affected by a reduction of their capability to carry out further calls.

Based on the dynamic AntiSPIT engine, the Eyeball AntiSPIT technology provides a complete SPIT prevention system for servers and end-point systems with the following features:

- SPIT Rating for Incoming Calls

Adds a SPIT rating tag to call message based on caller's calling rate, reputation and caller-callee relation to enable call filtering at the receiver. The SPIT-rating can be used by client applications such as the Eyeball SDK to indicate the nature of an incoming call.

- Caller Identification

Callers are identified using their SIP URI, SIP domain, IP address. Individual callers can be monitored as well as a group of callers from a domain or behind a firewall or NAT device.

- Challenge/Response Mechanism

The server uses a challenge/response mechanism whenever the calling rate limit of a caller exceeds a predefined threshold. In this case, callers are challenged for manual input before a call invitation is forwarded to the callee.

- Interoperability with 3rd Party SIP Proxy Servers

Eyeball AntiSPIT Server can be configured to work with SIP proxies from Eyeball as well as other 3rd party vendors such as Cisco/Dynamicsoft, Nortel, Iptel and Ubiquity.

Client-Side Features

Eyeball AntiSPIT technology also provides the following client-side features.

- Parental Control

Parents can control service usage using filtering techniques such as calling rate limit, unique callee limit, total call duration, time-of-day, and call content monitoring (such as skin-tone filtering).

- SPIT coding scheme

Client applications may indicate good, suspicious or bad calls using green, yellow or red lights (or using different ring tones) respectively.



End-point protection example: SPIT notification using different colors informs about incoming calls

Integration with existing VoIP Infrastructures

The Eyeball AntiSPIT technology is fully SIP-compliant. On the server side, the Eyeball AntiSPIT technology is already integrated into the latest version of the Eyeball Video Communication Server. Furthermore, the stand-alone AntiSPIT Server is available to support existing SIP-based VoIP infrastructures. The stand-alone AntiSPIT Server interoperates with a wide variety of different SIP servers, including Eyeball Video Communications Server, Cisco/dynamicsoft, iptel.org SER, and others.

The client features such as parental control and SPIT-alerts using the coding scheme are available in the latest Eyeball SDK, making the SPIT-rating available in any client based on the SDK while remaining compliant and inter-operable with other standard-based SIP servers.

Conclusion

With increasing popularity of VoIP installations based on open standards using common Internet technology, the risk of being attacked and affected by VoIP SPIT if various kinds rises. This includes not only mass calling and scan attempts but also harassment and exposure to unacceptable content especially when using video phones. The problem does not only have impact on VoIP systems but may also spread to traditional PSTN via



gateways. Therefore, effective means for protecting VoIP installations from mass calling attempts, hacker attacks, and other threats are required.

With patent-pending Eyeball AntiSPIT technology, the previously described security problems are addressed, providing protection against VoIP SPIT of various kinds using a complete client and server package for SPIT protection and prevention.

About Eyeball Networks

Eyeball Networks is a world leader in VoIP and video telephony software for service providers and device manufacturers. Eyeball's patented Any-Bandwidth™ and Any-Firewall™ Technologies guarantee the best possible voice and video quality for every subscriber, over any Internet connection, across any firewall, and on any device. Eyeball's endpoint and server software supports more than 6 million VoIP and video telephony subscribers and 10 billion call minutes for more than 100 service providers in North America, Europe and Asia.

Founded in 2000, Eyeball Networks is a privately-held company headquartered in Vancouver, British Columbia. For more information, visit www.eyeball.com.

Global Offices

Corporate Headquarters

Eyeball Networks Inc.
500 - 100 Park Royal
West Vancouver, B.C.
Canada, V7T 1A2
Phone: 604.921.5993
Fax: 604.921.5909

Regional Offices

USA
451 37th Street
New York, NY 10016
Phone: 646.428.5383

Japan
Tamachi East 803
2-16, Shibaura
3-chome, Minato-ku
Tokyo
Phone: +81 (3) 5440-4533
Fax: +81 (3) 5440-4533

United Kingdom
1A Orton Lane
Wombourne
Wolverhampton
WV5 9AN
Phone: +44 (0) 560 043 3364
Fax: +44 (0) 870 762 6001

Contact Eyeball Networks today for a live demonstration of our soft clients and servers.



Sales: sales@eyeball.com
Support: techsupport@eyeball.com

Standards and Codecs

A key to Eyeball's success in providing the industry's highest call completion is the intelligence at the endpoints which discovers the type of firewall(s) in use and for smart prediction of address and ports that can be used to complete a VoIP or video call.

Eyeball endpoint and server software is fully compliant with IETF standards and drafts such as SIP and SIMPLE. Eyeball Any-Firewall™ Technology uses standard protocols including STUN, TURN and ICE for exchanging connection information (such as address and port options) for completion of voice and video calls.

- ❑ RFC 3261 (SIP: Session Initiation Protocol)
- ❑ RFC 3665 (SIP Basic Call Flow)
- ❑ RFC 2617 (HTTP Authentication: Basic and Digest Access Authentication)
- ❑ RFC 3428 (SIP Extension for Instant Messaging)
- ❑ RFC 3263 (Locating SIP Servers)
- ❑ RFC 2327 (SDP: Session Description Protocol)
- ❑ RFC 2787 (DNS SRV)
- ❑ RFC 2190 (RTP Payload for H.263 Video Streams)
- ❑ RFC 3264 (Offer/Answer Model with SDP)
- ❑ RFC 3550 (RTP Protocol for Real-Time Applications)
- ❑ RFC 2833 (RTP Payload for DTMF Digits, Signals)
- ❑ RFC 3489 (STUN - Simple Traversal of User Datagram Protocol Through Network Address Translators)
- ❑ RFC 3920 (Extensible Messaging and Presence Protocol (XMPP): Core)
- ❑ RFC 3921 (Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence)
- ❑ Voice codecs: G.711, G.729A, GSM 6.10, iLBC, Speex, Speex-wb
- ❑ Video codecs: H.263, H.264, MPEG-4 and EyeStream