

Voice Printing And Reachability Code (VPARC) Mechanism for prevention of Spam over IP Telephony (SPIT)

*Vijay Radhakrishnan
&
Ranjith Mukundan*

*Wipro Technologies, Bangalore, India
Email: {radhakrishnan.vijay, ranjith.mukundan}@wipro.com*

2nd ETSI Security Workshop: Future Security
16-17 January 2007 - Sophia-Antipolis, France

Agenda

- **Introduction To Voip Spam (SPIT)**
- **Mechanisms to counter Voip Spam**
- **VPARC Architecture**
- **Way Forward and Conclusion**



Introduction To Voip Spam (SPIT)

What is Spam?

- ▶ Spam, in the context of electronic mail (e-mail), is any message that is transmitted to a large number of recipients, some or all of who have not explicitly and knowingly requested for this information
- ▶ VoIP networks, using the public Internet, are also subject to similar vulnerabilities as e-mail
- ▶ With the expected growth in VoIP deployments in the open Internet, there is a huge incentive for telemarketers to spam users with unsolicited information
- ▶ Using VoIP, telemarketers can send messages to thousands of addresses at a time, rather than tying up a single phone line to make one call

Impact Of VoIP Spam

➤ Voice Mailboxes

- The biggest likely impact of VoIP spam (SPIT) will be on voice mailboxes
- Mailboxes will record every message they receive, while a human answering the phone is likely to hang up within a few seconds after realizing that it is a spam call

➤ Automata

- A single Automata device can generate messages to multiple users simultaneously
- The transport cost will be miniscule over the internet making the problem more magnified and global in nature

➤ Use of SIP

- The use of the Session Initiation Protocol (SIP) that natively supports Presence, potentially means that a spammer can be aware of the availability of a user before spamming him
- Spoofing of insecure SIP messages can lead to Denial of Service kind of attacks

Types of VoIP Spam

➤ Call Spam

- Call spam is defined as a bulk unsolicited set of session initiation attempts (i.e., SIP INVITE requests) by the spammer to establish a communications session with the user.
- If the user answers, the spammer relays the “spam” to the user.

➤ IM Spam

- IM Spam is defined as bulk unsolicited set of instant messages, whose content contains the message that the spammer is seeking to convey.

➤ Presence Spam

- This type of spam is similar to IM spam. It is defined as a bulk unsolicited set of presence requests in an attempt to get on the "buddy list" of a user in order to send IM or initiate other forms of communications.



Mechanisms to Counter Voip Spam

Mechanism to counter VoIP Spam

➤ Black Lists

- A spam filter will maintain a list of the addresses and domain names of potential spammers
- Each user in the network will have a black list and calls originated from a black listed entity are rejected

➤ White Lists

- White lists are quite the opposite of black lists.
- White lists maintain a list of callers that the user is willing to accept calls from.
- Only those callers that are in the white list of the user are allowed to make calls to the user.

➤ Identity Assertion

- It is possible to securely identify the identity of a sender of a SIP message.
- Using SIPs http based digest authentication mechanism each SIP domain can authenticate its own users.
- When a domain has authenticated the identity of a user, it relays a message from that user to another domain.

Limitations of Existing Mechanisms

- A spammer in the Black List of the User can change his or her identity and launch a spam attack on the user
- A genuine caller who is not in the White List of the user, will never be able to call the user
- Each of these mechanisms is effective in countering a particular call spam scenario but, in isolation, may be ineffective in a different scenario
- Using a combination of VoIP spam prevention methods is more effective in spam control.



VPARC Architecture

VPARC Architecture for VoIP Spam Prevention



- VPARC uses mechanisms like White lists, Black lists and Identity Assertion in combination for VoIP Spam prevention
- In addition to these mechanisms, we propose to use Reachability Code and biometrics like Voiceprinting to counter VoIP spam.

▪ Reachability Code

- The Reachability Code (RC) is a code that is used along with the SIP URI to route calls to the user
- If a user's address (RC+URI) is compromised, the user will not have to change his SIP URI, and can change the RC only
- If the RC is changed, a potential spammer needs to get hold of the new RC to spam the user

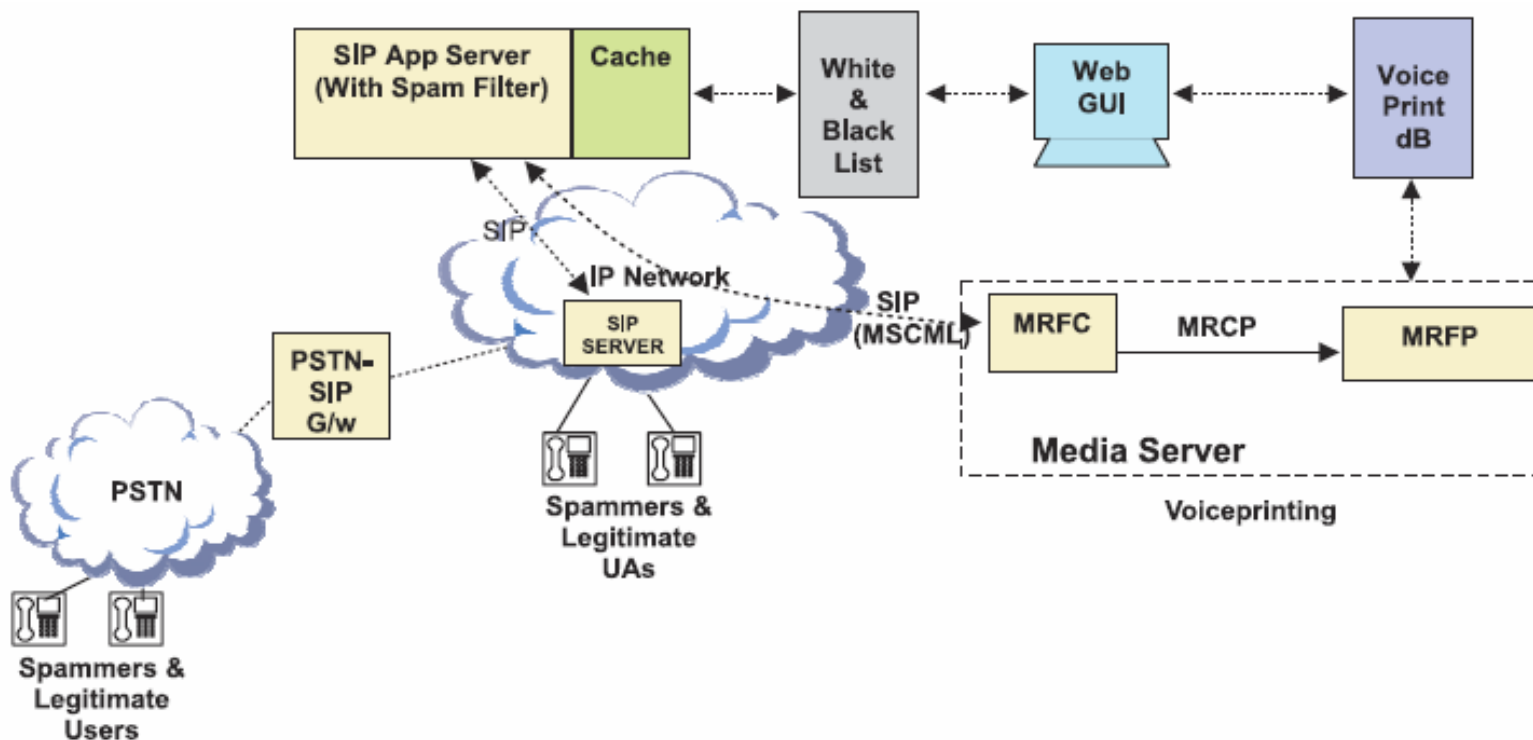
Uniform Resource Indicator(URI)	Reachability Code (RC)
bob@biloxi.com	1234
alice@example.com	4567

▪ Voiceprinting

- Voiceprint refers to a sample of speech that has been converted to a form that a voice biometrics system can analyze to verify the identity of the caller
- The system then performs a one-to-one comparison between the captured voiceprint (of the caller) and the stored voiceprint to identify a legitimate caller
- VPARC uses Voiceprinting to validate the caller

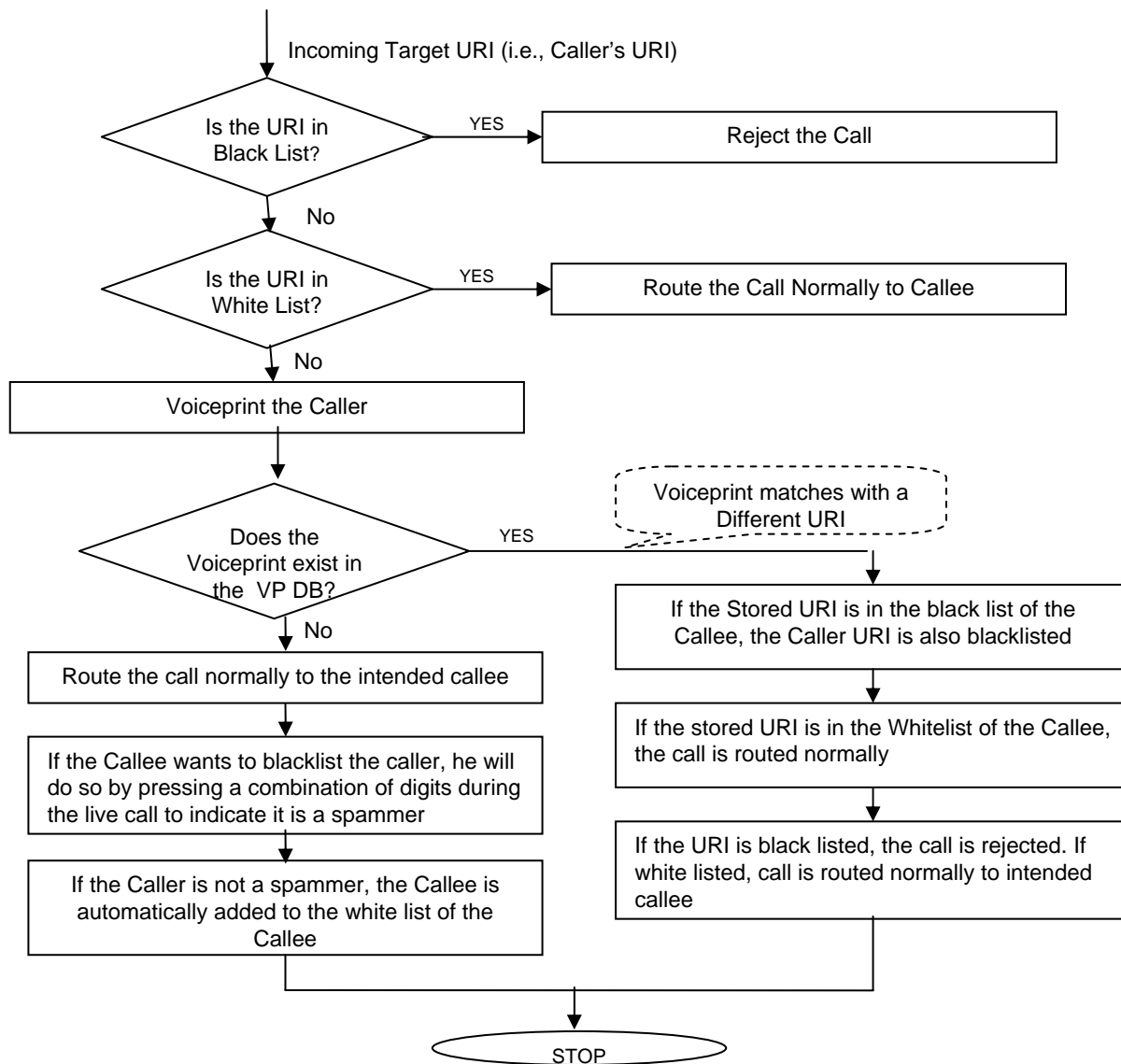
Voiceprint	Uniform Resource Indicator(URI)
<voiceprint of Bob>	bob@biloxi.com
<voiceprint of Alice>	alice@example.com

VPARC Architectural Model

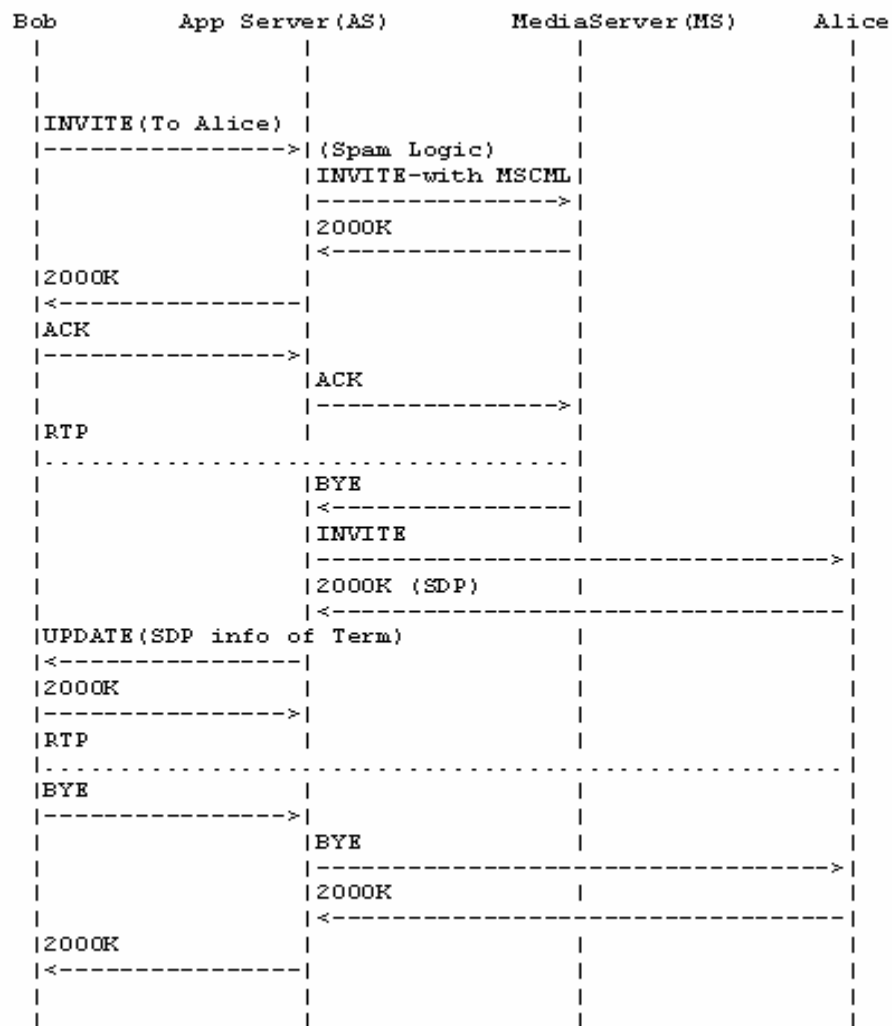


MRFC – Media Resource Function Controller
 MRFP – Media Resource Function Processor
 MSCML – Media Server Control Markup Language
 MRCP – Media Resource Control Protocol

Voip Spam Call Flow – Decision Chart

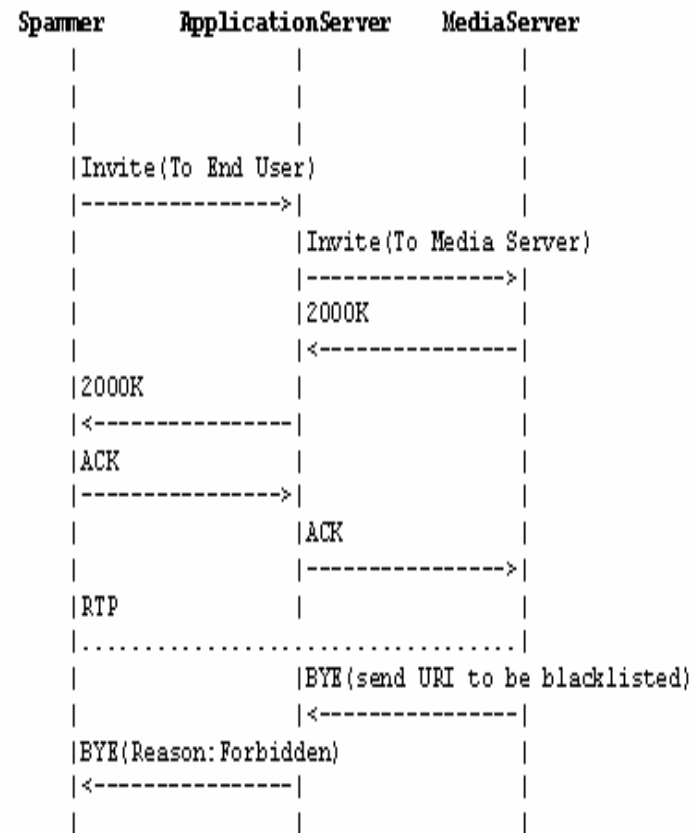


SIP Call Flow for Voiceprinting



Some Spamming Scenarios-Spammer calls from a Different URI

- The spammer, who has been black listed, calls from a new or assumed URI
- The RC check will pass and since there will be no entry in either the black or the white list, the call will be routed for Voiceprinting
- The voiceprint that has been generated is compared with all other voiceprints for the particular callee
- Since the caller was originally in the black list of the callee, the voiceprint will match, but would have been recorded against a different URI
- The new URI will also be black-listed





Future Work and Conclusion

VPARC-Way Forward

- We have proposed this architecture to key stakeholders in Standards bodies and we are currently working on an IETF draft based on VPARC
- We are also building a Proof-of-Concept Solution around VPARC in our Lab to demo it to various Operators and Service Providers who may be interested in deploying a similar solution.
- The existing solution uses Voiceprinting, which is an expensive technology. We are currently investigating the applicability of Presence-based mechanisms to counter Voip Spam

Conclusion

- Spam can pose a huge threat to the success of VoIP
- As the number of deployments increase, the risk posed by VoIP spam is huge.
- In this presentation, we have analyzed the kind of vulnerabilities in a VoIP network that are likely to be exploited by spammers
- We have discussed various mechanisms to counter VoIP spam and proposed the VPARC architecture that uses a combination of these mechanisms to effectively counter VoIP spam
- The only way to successfully counter Voip Spam is to be ready for it when it happens!!!