Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 24, 2008

P. Mutaf
March 23, 2008

Humanresolver: an introduction and model of operation
draft-mutaf-humanresolv-00.txt

Status of this Memo

Abstract

This document introduces "humanresolver": a peer-to-peer contact manager application.

Table of Contents

1. Introduction 3
2. Two modes of humanresolver 3
2.1. Face-to-face mode 3
2.2. Distant mode 3
3. Controlling the inbound path 4
4. Security considerations 4
5. IANA Considerations 5
6. Conclusion 5
7. Acknowledgements 5
8. References 5
Author's Address 5
Intellectual Property and Copyright Statements 6

1. Introduction

"Humanresolver" is the name of a contact management application. Using humanresolver, users set IPsec security policies, sign certificates, distribute SIP URIs, or other identifiers e.g. Mobile IP(v6) home addresses, DNS names etc., "under user control". The main goal of humanresolver is to allow for distribution (not publication) of user contact information while efficiently fighting SPIT (SPam over IP Telephony) and help establishment of IPsec secure channels. A user may want to distribute contact information on a forum, for example, to sell an item or ask for help, and remove the communication channel when done or upon arrival of SPIT. In human resolution, unlike a traditional phonebook, phone numbers are not published. Instead, a point-to-point secure communication channel is established with the target user, if (s)he accepts. Instead of their phone numbers, the users can publish their to be defined "humanresolver URIs" on the web or on presence services. This paradigm is very effective against SPIT. Since there is a point-to-point channel between each user, the cancellation of one channel has no impact on others. This scheme is analogous to but more secure than disposable e-mail addresses scheme (against SPAM) where a user distributes a different e-mail address to each contact and disable it when spam arrives.

2. Two modes of humanresolver

2.1. Face-to-face mode

In this mode, two mobile phone users have face-to-face contact and wish to exchange their contact information. One of the users enters or clicks on the published name or pseudo of the destination user (published on a local presence service). The two hosts detect each other, perform mutual authentication using a short authentication string [SAS] and sign each other's certificate and possibly exchange a symmetric key. No certification authority (CA) is needed for this mode.

By signing each other's public key, the hosts contribute to a web of trust pattern that is potentially useful in the distant mode of humanresolver. The face-to-face mode is an important existing model. Humanresolver takes this opportunity for better securing its distant mode.

2.2. Distant mode

In this mode, the target user publishes his/her human resolution URI on the web or a presence service in order to receive useful incoming

sessions. The initiator user clicks on the puslished humanresolver URI and the initiator humanresolver application is launched. A query is sent to the destination host which displays a message:

(name) wants to add you to his(her) contact list.
Accept? [YES/NO]"

By pushing on the YES button, the target user can accept the incoming human resolution request. The two phones will exchange SIP URIs, home addresses, IPsec policy information, etc. Human name certification will be required in this mode. Web of trust models or certification authorities can be used. Or, security associations can be accepted at one's own risk. Upon arrival of SPIT, the security association can be removed upon the target user's command.

In this mode the target host may display the above message only if it receives a valid certificate. Alternatively, the target host may return a CAPTCHA and only upon receipt of the correct solution to the CAPTCHA it can display the above message. This would prevent an initiator user from continuously annoying the responder user by making display the above message with bogus requests.

3. Controlling the inbound path

In addition to controlling incoming session authorizations, the users can control the inbound path for communication. Two hosts having exchanged home addresses through human resolution will not need SIP infrastructure e.g. SIP triangle or trapezoid in order call each other. Routing will be handled by Mobile IP. The hosts may even avoid exchanging Mobile IP home addresses if the contact is not supposed to be kept permanently. This feature can help the target user better preserve privacy and tranquility against some type of users. The target user cannot be called regardless of location because the initiator is not given a home address. (S)he can only be called "now", at this location, for example at the office. Each time the initiator user needs to contact the target host, (s)he will need to visit the web page where the target humanresolver URI is published and make another request.

4. Security considerations

TBD.

5. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

6. Conclusion

This document described the basic motivations and theory of operation of the humanresolver contact manager.

7. Acknowledgements

TBD.

8. References

[SAS] Vaudenay, S., "Secure Communications over Insecure Channels Based on Short Authenticated Strings", 2005.

Author's Address

Pars Mutaf

Email: pars.mutaf@gmail.com

Full Copyright Statement

Intellectual Property