Network Working Group
Internet-Draft
Expires: September 18, 2008

Pars Mutaf

March 17, 2008

IKEv2 extensions for combating SPIT on mobile hosts
draft-mutaf-spikev2-01.txt

Status of this Memo

Abstract

This document describes IKEv2 extensions for combating SPIT on mobile hosts.

Table of Contents

1. Introduction

"Voice over IP systems, like e-mail and other Internet applications, are susceptible to abuse by malicious parties who initiate unsolicited and unwanted communications called SPIT (SPam over Internet Telephony). Telemarketers, prank callers, and other telephone system abusers are likely to target VoIP systems increasingly, particularly if VoIP tends to supplant conventional telephony." -- from Wikipedia entry on VoIP spam, March 2008.

[RFC5039] provides a detailed analysis of the SPIT risk, reviews the existing approaches for e-mail spam and provides guidelines for combating spam over IP telephony.

SPIT is likely to be very annoying on cell phones carried in one's pocket during the day. Each time SPIT arrives the user will be notified for a useless, annoying and potentially harmful message or call. This document describes IPsec solutions and IKEv2 extensions for combating SPIT on cellular hosts.

2. Solutions

This section describes two solutions: weak and strong. The described solutions are extensions to the Internet Key Exchange (IKEv2) protocol [RFC4306].

2.1. Weak

A solution to SPIT is to require an IPsec SA (Security Association) before a correspondent opens a session with a target SIP URI. If later the correspondent turns bad and sends SPIT, the target cell phone can remove the SA.

To prevent an attacker from repeatedly establishing SAs with the target host and sending SPIT, the initiator can be requested to solve a hard challenge. IKEv2 supports cookies which can be used to prevent an attacker from spoofing IP addresses. When fighting against SPIT, one has an important advantage: the sender, if legitimate, is necessarily a human. Consequently, Turing tests known as CAPTCHA can be used [CAPTCHA]. The IKEv2 responder can return a CAPTCHA to check if IKEv2 is initiated by a human. Difficult CAPTCHAs can also be used to challenge a malicious human. If the initiator user does not return the correct solution to the CAPTCHA, IKEv2 will not proceed normally and an SA will not be established. Additional defenses include adaptively increasing the difficulty of the CAPTCHA, and temporarily blacklisting the attacker's IP address.

If the SPIT has commercial purposes, the attacker is unlikely to continuously send the same advertisement to the same target user. A commercial attacker would rather target a large number of hosts and send the same advertisement to each of them. The above defense can defeat commercial attacks, since the attacker will need to solve a large number challenges coming from each target host. A September 2006 Slashdot article on CAPTCHA reports how "data entry specialists" solve captchas for $0.60 per hour for 50 hours a week [SLASHDOT]. The popularity of CAPTCHAs does not seem to be affected, however. Popular web sites, e.g. Google and Yahoo! still employ this defense to protect their resources.

2.2. Strong

This approach extends the above defense with strong identities and target user's approval. The target user may want to receive incoming sessions or short messages from known people only. Or, the initiator user may be unknown but the target user may have an idea who (s)he is. A security association may be established with unknown users as well, however in any case the target user requires a certified identity of the initiator.

Along with a CAPTCHA (as described above), the target host sends a human name certificate request. The initiator returns the required certificate along with a solution to the CAPTCHA challenge. If the CAPTCHA solution is correct, the target host displays the initiator's human name and asks for permission to create an SA:

"Michael Knight wants to connect.
Accept? [YES/NO]"

If accepted by the target user, IKEv2 will proceed and an IPsec SA can be established with the target cell phone. Regarding the validity of the initiator's certificate, there are two possible approaches:

a) If the certificate is invalid, stop IKEv2.
   Else continue.
b) If the certificate is invalid, notify the
   target user and wait for user decision.
   If accepted, continue. Else stop IKEv2.

The advantage of (a) is that attackers cannot make bogus requests disturbing the target user with messages asking for user permission. On the other hand, valid human name certificates may not be always available. Some users may choose (b) notifying the target user and wait for user decision. In this case, however, an attacker can send continuous bogus requests forcing the target host frequently display

the above message, annoying the target user. This attack can be defeated by requesting the initiator user to solve a CAPTCHA before his request can be displayed at the target host's screen. The difficulty of the CAPTCHA can be adaptively tuned by the target host.

An important point to note here is that by solving a CAPTCHA, the attacker will not obtain anything. The target user can always reject the connection attempt, if the initiator is unknown, or a known person is being impersonated. This is an important difference from the weak defense (above) where an attacker can send SPIT by solving a CAPTCHA.

3. Off-line protection

In current cellular systems, when the target device is off-line or busy, the calling party can leave a voice message in a message box. The message is forwarded to its destination when the target phone is up and available again. Similarly, text messages are buffered in the system, and delivered later when the target phone is ready. The message box may be filled with spam voice messages and text messages.

In the Internet, e-mail can be used for voice and text messages. When an initiator host successfully established an IPsec SA with a target host, the target host can return an e-mail address. The target host should also sign and return a public key certificate of the initiator. This will prove that the initiator is authorized to leave messages to the indicated mailbox. When the target host is off-line or busy, the initiator can detect it and send a locally recorded voice file to the indicated e-mail address. When the target host is up and available, it will fetch the e-mails found in the mailbox, or the e-mails will be pushed to the mobile host.

The certificate issued by the target host proves authorization to send e-mail to the target host's mailbox. If the initiator turns bad and sends SPIT to the target host's mailbox, its certificate should be revoked until it expires. The certificate lifetimes should not be too long. They should be prediodically updated by the target host. For example, each time a legitimate communication takes place, the target host can issue a new and fresh certificate replacing the old one.

4. IKEv2 extensions

In its current form IKEv2 does not support CAPTCHA challenges, nor asking responder user's permission to proceed. 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. Security Considerations

TBD.

7. Conclusion

This document decribed IKEv2 (Internet Key Exchange version 2), extensions for combating SPIT (SPam over Internet Telephony).

The described defense forces an initiator user to solve a CAPTCHA for establishing an IPsec Security Association (SA). Legitimate users will solve only one CAPTCHA and continue to profit from the same SA during future sessions. The attacker will need to solve a different CAPTCHA for each SPIT that s(he) sends to the target host. When SPIT arrives from a source address, the corresponding SA will be dropped upon the target user's command. This defense (although weak) puts the legitimate users in a much more advantageous position than malicious ones.

With the strong defense, the attacker needs to solve a CAPTCHA, and even after returning the right anwser the attacker is not certain that the SPIT reached the target user. The target user may reject the request because (s)he has no idea the sender is. Moreover, if the attacker's certificate is valid (otherwise SPIT cannot be sent) the attacker's identity will be revealed and black listed by the target phone.

8. Acknowledgements

TBD.

9. Normative References

[CAPTCHA] Ahn, L., Blum, M., and J. Langford, "Telling Humans and Computers Apart Automatically", In Communications of the ACM, February 2004.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC5039] Rozenberg, J. and C. Jennings, "Session Initiation Protocol (SIP) and SPAM", RFC 5039, January 2008.

[SLASHDOT] http://it.slashdot.org/article.pl?sid=06/09/06/1217240, "Will Solve Captcha for Money?", September 2006.

Author's Address

Pars Mutaf

Email: pars.mutaf@gmail.com

Full Copyright Statement

Intellectual Property