The SIP Identity Baiting Attack
draft-kaplan-sip-baiting-attack-02

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 22, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
The SIP Identity Baiting Attack February 2008

Abstract

This document identifies a potential SPIT and Phishing attack, which subverts the RFC 4474 SIP Identity and RFC 4916 Connected Identity mechanisms in a particular way. The attack is termed "Baiting", as it uses a RFC4474-signed call as the bait for malicious use.

Table of Contents

1. Introduction................................................2
   1.1. Background.............................................3
2. Terminology................................................3
3. Applicability...............................................4
4. Overview of the Attack....................................4
5. Harvesting Signed Invites..................................5
6. RFC-4474 Cut-Paste Protection.............................6
7. Baiting with Offer-less Invites.............................7
8. Baiting with ICE............................................7
9. Baiting with SRTP.........................................7
10. Baiting with non-INVITE Requests..........................7
11. Attack Success Conditions................................8
12. Possible Solutions?.......................................8
   12.1. SIP Identity and SIP Connected Identity.............8
   12.2. Secured Media with a Secret........................9
13. Security Considerations..................................9
14. IANA Considerations....................................9
15. References..............................................9
   15.1. Informative References................................9
Authors’ Addresses.............................................10
Intellectual Property Statement.............................12
Full Copyright Statement.....................................12
Acknowledgment.............................................12

1. Introduction

SIP Identity, defined in [RFC4474], defines a mechanism for originating domains to sign SIP requests with a certificate, in order to prove the legitimacy of the From identity and the request’s body content. The motivation of the work derived from the need to provide a form of cryptographically strong end-to-end (or end-domain to end-domain) identity, in order to avoid malicious use of identity fraud.

While not specifically called out, many people consider the [RFC4474] mechanism as useful for preventing SPIT and Phishing attacks, because strong identity is a basis for many anti-SPIT
techniques [SIP-SPAM]. This draft describes a form of attack which shows that is not the case.

Furthermore, [RFC4916] defines a way to use the same Identity mechanism to perform called party identification, by issuing a re-INVITE or UPDATE request from the called party to the caller. This draft describes a way to mis-use that mechanism to aid in the attack.

It should be noted that neither [RFC4474] nor [RFC4916] claim to prevent this form of attack, nor in fact is Baiting an attack on the mechanisms themselves. It uses the mechanisms for malicious use, and shows that the mechanisms should not be assumed to provide benefits they do not. Lastly, one of the motivations in writing this draft was to show that one does not need to truly be a man-in-the-middle in order to perform a cut-paste form of attack such as Baiting.

1.1. Background

SIP [RFC3261] has a transitive trust model, whereby SIP requests get routed through various intermediaries. In this model, the initiating User Agents (UAs) must generally rely on the intermediaries to be secure. Such a trust model has many security issues, one of which is identity proof. As in email, if the identity of the sender of a message cannot be secured, various forms of impersonation attacks are possible.

Two very common issues in email today are SPAM and Phishing attacks, which both benefit from impersonation. For SIP-based applications, SPIT (SPAM for Internet Telephony) is not yet a serious problem, due mostly to the early stage of SIP deployment, a closed service model, and fees for use. As it grows in popularity and decreases in cost, however, its potential for attracting SPIT will grow.

[RFC4474] follows a similar general model as [DKIM] for source-based identity authentication, but the resulting symptoms caused by some of DKIM’s weaknesses has greater importance for SIP as a real-time session-setup protocol than Email does. SPAM, for example, would be far less tolerated for phone calls than they would for email, even if the called party ignored the call but the phone rang.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. The terminology in this document conforms to RFC 2828, "Internet Security Glossary".
3. Applicability

This draft applies to the [RFC4474] SIP Identity and [RFC4916] Connected Identity mechanisms.

4. Overview of the Attack

The general form of the attack is as follows:

1. An attacker, Bob, is registered at a typical [RFC3261] compliant domain: example.net. Bob wishes to attack alice@example.com.
2. Bob "harvests" an [RFC4474] signed request from a legitimate party, such as Bank. This can be done through various means, such as filling out a web form for the Bank to call him, leaving a voicemail, or whatever - or possibly using the [RFC4916] connected-identity mechanism, as described later in this document.
4. Bob terminates the call attempt from Bank with a failure response.
5. Bob takes the received SIP Invite request from Bank, inserts a Via and Record-Route header of his UA’s address, and changes the request-URI with a new target of sip:alice@example.com, the ultimate victim of the attack. Bob may also change the From tag, delete the received Via’s, and/or possibly insert a History-Info header.
6. Bob sends the Invite through his domain example.net, or directly to example.com, or through another domain.
7. The signed request is routed based on the request-URI, eventually leading to Alice’s Identity verifier.
8. Alice’s domain receives the request, and verifies the [RFC4474] identity signature. In the previous steps, Bob has not changed anything which was signed by [RFC4474], so the validation succeeds. Note that the To URI will most likely be sip:bob@example.net, but per [RFC3261] Alice’s domain does not verify that the To domain is the same as Alice’s domain - nor could it, because the request may have simply been forwarded through re-targeting, which is legitimate.
9. Alice’s phone rings, with Bank appearing as the source caller. At this point, Bob has already succeeded in annoying Alice, because her phone rang, and she thought it was Bank.
10. Alice picks up the phone, which sends a 200 ok response to Bob.
11. Bob receives the SDP answer in the 200 ok, which tells him where to send media to Alice. Bob sends an ACK to Alice.
12. Bob then sends his SPIT audio RTP to Alice, possibly spoofing the IP Address and port in the SDP offer sent by Bank. Bank will not be sending RTP itself, because it does not get the 200 ok, and (in step 4) Bob terminated the call from Bank.

13. At this point Bob is successfully SPAM-ing Alice. Alice may send media to Bank, but since Bob terminated the call from Bank (in step 4), Bank discards/ignores the media from Alice.

14. Alternatively, Bob may attempt Phishing by inserting a Call-Info header with a HTTP URL or even a DATA URL, and the audio may tell Alice to click on the link or view the DATA URL content. Alice receives a cryptographic assertion that the call is from Bank, and thus the phishing attack has a higher chance of success.

Note that this form of the attack creates one-way media, from Bob to Alice, which Alice believes is from Bank. Bob can use the one-way media to announce an advertisement, such as:

"Your Bank urges you to vote for <candidate> during the upcoming election. Thank you and have a nice day."

Or Bob might use the one-way audio for phishing, such as:

"This is a recording from your Bank. Your account has been compromised. Please call us, at <attacker’s phone number>, to restore service to your bank account. Thank you and have a nice day."

When Alice calls the attacker’s phone number, the attacker will now have bi-directional audio with the victim.

5. Harvesting Signed Invites

There are several ways in which an attacker, Bob, can try to harvest multiple [RFC4474] signed Invite requests for malicious use:

1. Bob can have Bank call him, by submitting web contact forms, leaving voicemail, etc.

2. If Bank calls Bob, Bob can issue 3xx redirect responses to redirect the call request to another alias account, or even to himself again. This may even yield new Call-Id’s for each redirected request, and minimally new CSeq values - each of these will have a valid [RFC4474] signature.

3. If Bank calls Bob, and Bank supports [RFC4028] Session Timers, Bob can respond with a low Session-Expires header duration (e.g., 90 seconds), with a refresher=uac parameter, and an Allow header which does not include UPDATE as an allowed Method, in an attempt to get Bank to issue signed re-INVITEs continuously and often.
4. Bob can make a SIP call to Bank, such as Bank’s 800-number IVR system, expecting Bank to support [RFC4916] Connected Identity. Bob can send an Allow header which does not include UPDATE as an allowed Method, in an attempt to get Bank to issue a re-INVITE to prove its identity.

5. For calls initiated by Bob, Bob could include the [RFC4028] ‘timer’ Supported option tag and Session-Expires header of short duration (e.g., 90 seconds), with a refresher=uas parameter, in order to get Bank to issue re-INVITE’s continuously and often.

6. Bob could try to passively monitor legitimate, unencrypted, SIP traffic.

7. Bob could try to become a "Man-in-the-Middle", for example by compromising a legitimate Proxy.

Note that any signed INVITE, whether within a dialog or not, is potentially useful for performing a Baiting attack. [RFC4474] does not sign the To-tag, and thus it can simply be removed for re-use as a "new" INVITE. Stateful verifiers may or may not detect such re-use. And Bob can simply send them to different target domains, to avoid hitting the same verifier.

Even if Bob sends multiple such INVITEs, with the same Call-Id, to the same target domain, [RFC4474] is not explicit about how a Verifier should behave. Each harvested request would have a unique CSeq value, and thus unique signature, and not be detected as a strict replay attack per [RFC4474]. It is not clear how it really could be detected as a replay, either, given the need to support legitimate signed re-INVITEs within a dialog, and dialog matching based on Call-Id and tags (not Call-Id alone).

6. RFC-4474 Cut-Paste Protection

It is important to note that [RFC4474] signs the Call-Id in an attempt to prevent such cut-paste attacks. The assumption is that the verifying domain keeps track of the call-id’s for the duration of the Date interval (typically 1 hour), and does not allow a duplicate request using the same Call-Id. This Baiting attack sends the request to a domain other than the one in the To-URI, and thus one harvested [RFC4474]-signed INVITE can be sent to numerous target domains.

Interestingly, Bob can use one of the listed harvesting techniques within a dialog or through 3xx redirects, to get additional signed requests to use against different users of the *same* target domain. Thus Bob could attack multiple users in the same target domain from one [RFC4474] call from or to Bank. Furthermore, if verification is performed by the end UA’s and not by a centralized verifier system
for the end-domain, this attack would succeed against *all* users of that domain from one harvested INVITE (because the end UAs would not be able to protect each other from cut-and-pasted Call-IDs).

7. Baiting with Offer-less Invites

If Bank were to generate an Invite without SDP, the attack is still possible, but even more severe because the attacker (Bob) can end up with a bi-directional media call. Bob would be able to send media on Alice’s SDP offer in her response, and Bob could create his own ACK with his SDP answer. If Alice expects an identity-signed ACK, Bob could even answer Bank’s call and use Bank’s signed ACK in the same way as the Invite. Note that [RFC4474] provides no mechanism to determine when ACKs need to be signed, and since an ACK cannot be responded to, Alice cannot really reject it either - it would be silently ignored.

8. Baiting with ICE

The NAT traversal mechanism defined in [ICE] would seem to aid the attacker. The password and username fragment are signed by [RFC4474], but they will be clearly viewable to the attacker, and thus the attacker should be able to generate STUN connectivity checks using them, impersonating the legitimate caller. We believe this would mean ICE would actually enable the attacker to achieve bi-directional media, for the malicious call. [This is TBD, pending review by an ICE expert (a glaciologist?)]

9. Baiting with SRTP

The Baiting attack is just as successful with the [RFC4568] security-descriptions key exchange mechanism, because the keys are in cleartext for the attacker. The attacker can thus generate the SRTP packets to the victim. For [DTLS-SRTP], coupled with [DTLS-SRTP-FRAMEWORK], the fingerprint being signed prevents a Baiting attack from succeeding, because the attacker cannot successfully modify the fingerprint in the [RFC4474]-signed SDP.

10. Baiting with non-INVITE Requests

It should be clear that the main focus of the Baiting attack outlined in this draft is the INVITE request, however one can apply Baiting to other requests. All SIP requests outside of a dialog are routed based on the request-URI or Route headers, and thus any harvested request can be cut-paste to a new target. However it is harder to harvest such requests in general, and to do so in such a way that it provides any real gain to cut-paste them, other than for annoyance purposes.
11. Attack Success Conditions

What makes the attack successful are the following issues with the [RFC4474] mechanism:

1) Requests in SIP are routed based on the Request-URI and/or Route headers, not the To-URI. The To-URI is signed, but it doesn’t prevent the request being sent elsewhere and accepted by parties other than that indicated in the To-URI. Email-based [DKIM] has a similar issue, but at least with email the To information is displayed, whereas it rarely is with SIP.

2) Unlike Email, where all of the sensitive content is contained in the body of the request, SIP is used as a rendezvous and session setup protocol for the sensitive content: the media. That is why [RFC4474] signs the SDP: in order to provide some protection for the ultimate content. But as this attack shows, it cannot truly do so alone.

3) [RFC4474] does not sign the Call-Info header.

4) [RFC4474] does not sign the tags of the request. While it provides no clear use to do so for initial requests (which have no To-tag), it would protect requests within a dialog. [RFC4916] simply re-uses the [RFC4474] mechanism, and thus would benefit from this as well.

12. Possible Solutions?

12.1. SIP Identity and SIP Connected Identity

The purpose of this draft is to outline a security issue with [RFC4474] and [RFC4916], not to fix it. However, we outline a few possible corrections to [RFC4474] to address parts of the attack:

1. Sign the Call-Info header. It is "sensitive" in a similar way as SDP or bodies.

2. Include the tags, or at least the To-tag, in the signed headers list. This would prevent harvested in-dialog requests from being re-used outside the dialog.

3. Clearly specify how Verifiers should act with respect to two signed requests of the same Call-Id+CSeq but different tags, vs. same Call-Id but different tags+CSeq should behave.

4. Possibly specify that UPDATE requests without bodies are not signed? Seems like a massive overhead for session-timers to sign such requests.
To address the general issue of request routing having nothing to do with the signed To-URI, one possible solution is to have the UAS or Verifier have a list of AoR's/To-URI's they are willing to accept requests for. In other words, if Alice's UAS or Verifier knew that only requests with a To-URI of "sip:alice@example.com", and whatever other aliases and lists/groups she is a member of, were allowed, then the UAS or verifier could simply reject baited requests. [in fact, such a thing is probably generally useful regardless of Identity signatures] This "access list" could be provisioned by Alice into her UAS, or her UAS could publish such information into the Verifier, or her UAS or Verifier could learn it from her Registrar through a subscribe package or config-framework, etc.

Such an access list mechanism would only work for native SIP users, however. One could not, for example, be able to create an access list for a SIP-PSTN gateway, since such gateways handle calls to any PSTN destination user. This may or may not be a good property to have for Identity verification, but it severely limits the usefulness of [RFC4474].

12.2. Secured Media with a Secret

For SIP methods involving media, such as an INVITE, the use of secure media with proof of possession of a secret (such as a private key) can prevent the Baiting attack. Examples of this include comedia-tls [RFC4572], [IDENTITY-MEDIA], and [E2E-SEC-MEDIA].

13. Security Considerations

The purpose of this draft is to identify a security issue.

14. IANA Considerations

None; this document is informational.

15. References

15.1. Informative References


The SIP Identity Baiting Attack

February 2008


Authors’ Addresses

Hadriel Kaplan
Acme Packet
71 Third Ave.
Burlington, MA 01803, USA
Email: hkaplan@acmepacket.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).