Response Identity and Authentication in Session Initiation Protocol

(draft-cao-sip-response-auth-00)

Feng Cao Cullen Jennings

August 2, 2005

Content

Introduction

- Current work for SIP security
  - Enhancements for SIP Request Identity
    - Jon Peterson and Cullen Jennings: *draft-ietf-sip-identity-05*
  - Certificate Management Service
    - Cullen Jennings and Jon Peterson: *draft-ietf-sipping-certs-02*
- Concerns about SIP Response
  - Identity
    - Who sends back the response?
    - Can the responder's identity be authenticated?
  - Authentication
    - Can the received response be trusted?
    - How to authenticate the received response?

Introduction

- Reasons for new methods

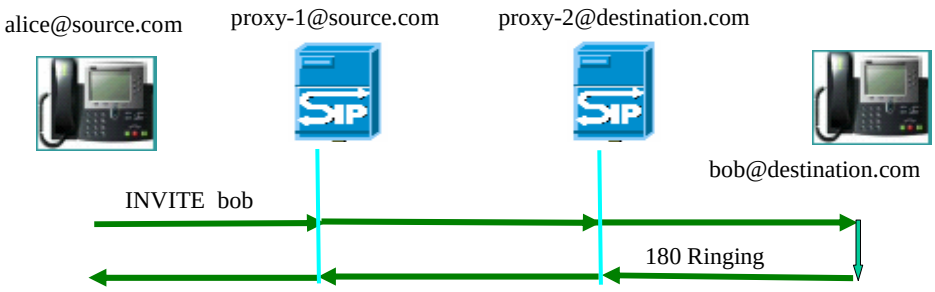
  Some reasons were brought up by *draft-ietf-sip-identity-05*
  - Few end-user certificates for TLS or S/MIME
  - Difficulties for Digest authentication for end-users
  - Random calls with no previous associations

Response Identity: Requirement

Some requirements for Response Identity

- The mechanism should be backward compatible
- The identity should be clearly specified in the header by the responder
- The identities of both UAs and proxies should be covered
- The integrity of SIP response should be covered along with the responder's identity

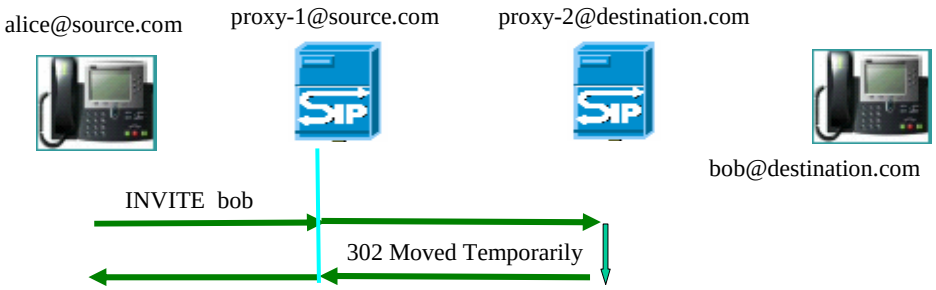
Response Identity: Overview



Responder: claimer=bob@destination.com;
verify-method=DAS;
Responder-Info: https://www.destination.com/certs
Identify: akfjiqiowrgnavnvnnfa2o3fafanfkfjakfjalkf203urjafskjfaf
Jprqiyupirequqpiruskfka

Note: *Domain-based Authentication Service (DAS)*

Response Identity: Overview



Responder: claimer=proxy-2@destination.com;
verify-method=DAS;
Responder-Info: https://www.destination.com/certs
Identify: jgaskljggjqvmvajfaskjfwioakfjiqiowrgnavnvnnfa2o3fafanfkfjak
fjalkf203urjafskjfafJprqiyupirequqpiruskfka

Note*: Domain-based Authentication Service (DAS)*

Response Identity: Syntax

Responder = "Responder" HCOLON responder-param
responder-param = claimer-param *(SEMI verify-param)
claimer-param = "claimer" EQUAL (name-addr / addr-spec)
verify-param = "verify-method" EQUAL ("DAS" / token)

Responder-Info = "Responder-Info" HCOLON responder-info (* SEMI responder-info-params)
responder-info = LAQUOT absoluteURI RAQUOT
responder-info-params = responder-info-alg / responder-info-extension
responder-info-alg = "alg" EQUAL token
responder-info-extension = generic-param

Example:
Responder: claimer=proxy-2@destination.com;
verify-method=DAS;
Responder-Info: https://www.destination.com/certs

Response Identity: Syntax

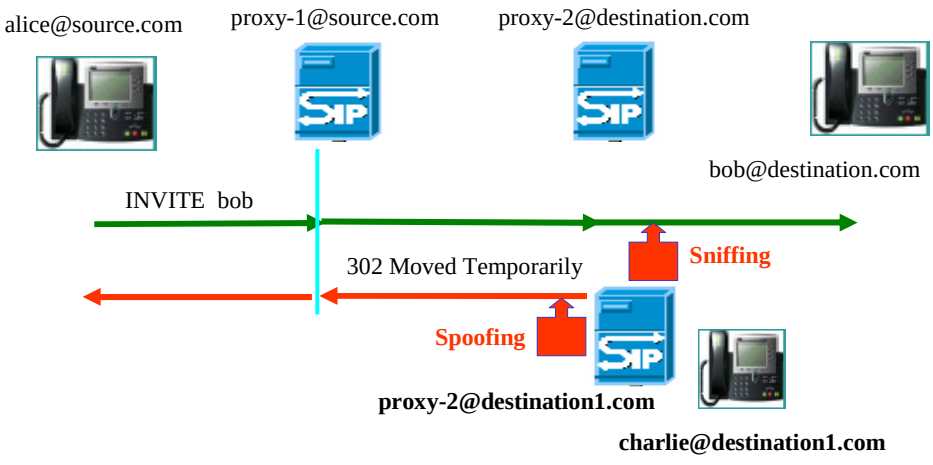
Identity = "Identity" HCOLON signed-identity-digest
signed-identity-digest = LDQUOT 32LHEX RDQUOT

Note: sha1WithRSAEncryption as described in RFC 3370
base64 encode the results as specified in RFC 3548 [8].

digest-string = addr-spec ":" addr-spec ":“
addr-spec ":" callid ":" 1*DIGIT SP method
":" SIP-Date ":" message-body

- addr-spec in To
- addr-spec in From
- addr-spec of claimer field in Responder
- callid from Call-ID
- the digits and the method from CSeq
- Date field
- body content of the message with the bits exactly as they are in the message (in the ABNF for SIP, the message body).

Response Authentication: Concerns

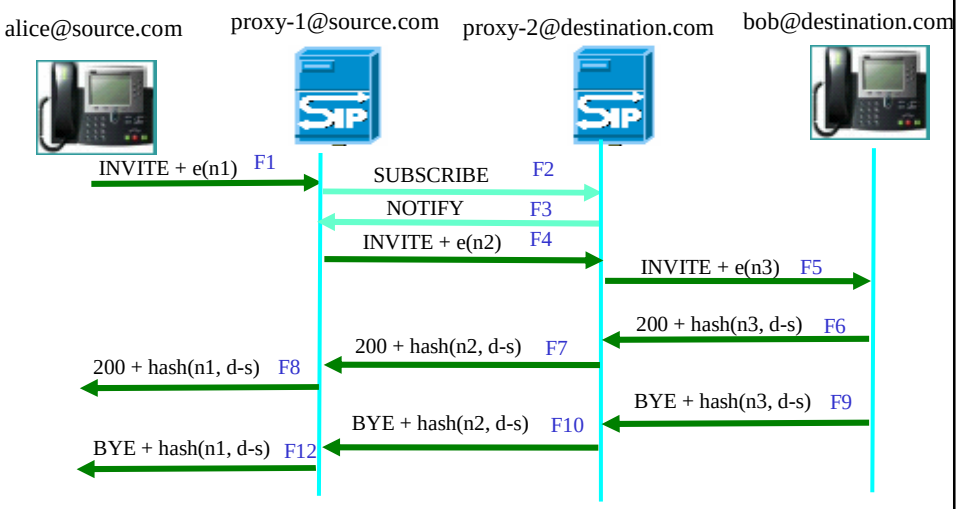


Response Authentication: Overview

Some requirements should be addressed:

- authentication between neighboring domains or nodes can be enhanced
- The mechanism should be simple
- Chain of SIP Response Trust (CSRT) can be built when this mechanism is applied on all the hops

Response Authentication: Overview



Response Authentication: Overview

- Indicate the challenge to the downstream node:
  - F1:

    Response-Authentication: *method="SharedKey";*
    nonce="nkfdowkjafaruqpjfaanqgqofmaklmcmhgq
    akjutygvcxdsgjgloruytetrkqqwqpoimzjubfcvdxer"
  - F4:

    Response-Authentication: *method="PublicKey";*
    nonce="jaskfnkfowjakqzalmjnbgvcfdxsyruiwojksnxjwrwwryuhg
    fdcvbnmkjhgfdxcvbnjfarqpjfanqgomaklmcmhgqp"
- Provide the digest of per-hop response from the down-stream node
  - F7:

    Response-Authorization: digest="qpowiuyetrgfhdjnueyhpazmcnbvhfgruiejdnqloutye
    wsxcdvmnhgblmwqaxdkjfuhgj"
  - F8:

    Response-Authorization: digest="qpowiuyetrgfhdjnueyhpazmcnbvhfgruiejdnqloutye
    wsxcdvmnhgblmwqaxdkjfuhgj"

Response Authentication: Syntax

Indicate the challenge to the downstream node:

Response-Authentication = "Response-Authentication"
HCOLON resp-authen-param
resp-authen-param = auth-method-param * (SEMI nonce-param)
auth-method-param = "method" EQUAL auth-method-enum
auth-method-eum = "DAS" / "SharedKey" / "PublicKey"
nonce-param = "nonce" EQUAL "nonce-value"

For example,

Response-Authentication: method="PublicKey";
nonce="jaskfnkfowjakqzalmjnbgvcfdxsyruiwojksnxjwrwwryuh
gfdcvbnmkjhgfdxcvbnjfarqpjfanqgomaklmcmhgqp"

Response Authentication: Syntax

Provide the digest of per-hop response from the down-stream node

Response-Authorization = "digest" EQUAL resp-author-digest
Resp-author-digest = LDQUOT 32LHEX RDQUOT

digest-string = status-code ":"
addr-spec ":" addr-spec ":" addr-spec ":"
auth-method-enum nonce-value ":"
callid ":" 1*DIGIT SP method ":" SIP-Date ":"
message-body

Note: status code of the response, addr-spec in To, addr-spec in From, addr-spec of claimer field in Responder, method and nonce in Response-Authentication, callid from Call-ID, the digits and the method from CSeq, Date field, body content of the message with the bits exactly as they are in the message (in the ABNF for SIP, the message body).

New Response Codes:

- *431 Failed Responder Identity*
  - Proxies might verify the identity of the responder and indicate the problem as early as possible
  - The originator might double-check
- *432 Failed Response Authorization*
  - Proxies might indicate the failure of per-hop authentication to prevent attacks
  - the per-hop authentication is needed before the received response with this code can be trusted.

Open Issues

- AIB as one verify-method for response identity?

  Responder: claimer=px2@destination.com; verify-method=AIB
  Responder-Info: https://www.destination.com/certification

- Nonce between neighbors for per-hop response authentication
  - per request vs. per session?
- Other mandatory algorithms besides rsa-sha1?
- Anonymity?

Summary

- New method for Addressing Response Identity
- New method for Addressing Per-hop Response authentication
- Enhancement of SIP Response Security
  - Identity of Responder
  - Chain of SIP Response Trust can be built
- Some open Issues