SIP WG meeting
73rd IETF - Minneapolis, MN, USA
November, 2008

Return Routability Check
draft-kuthan-sip-derive-00

Jiri Kuthan Jiri.Kuthan@tekelec.com
Dorgham Sisalem Dorgham.Sisalem@tekelec.com
Raphael Coeffic Raphael.Coeffic@tekelec.com
Victor Pascual Victor.Pascual@tekelec.com
Problem statement

- When someone is calling you, you’d like to be able to know the identity of the caller – “who are you?”
- But this is not always possible to determine – draft-elwell-sip-e2e-identity-important
- Are we comfortable enough to answer the question “are you calling me?” by determining:
  - whoever is calling me (even unknown party) can be reached at the address it is claiming in the From header field
Return Routability Check in a nutshell

- It is a simple “better-than-nothing“ approach to URI verification
  - End-to-end solution based on SIP routing
    - It leverages the location service retargeting
  - No trust models
  - No additional infrastructures apart from what it takes to route the INVITE message

- It is NOT a solution for the whole identity problem
  - It does not determine identity (“who are you?”), just the source URI of the call (“are you calling me?”)
Known Limitations

• It can at best confirm URI veracity. DERIVE cannot provide a refute claim
• Reverse Routability is known not to be available in many cases
  – unregistered phone, call forwarding, etc.
• Additional latency in call setup
Security Considerations

• Reliance on security of the Registrar, DNS and IP routing systems
• DoS opportunity with indirection
  – DERIVE allows attacker to drive other UAs to send DERIVE requests to a victim
• Privacy
  – In the absence of some sort of authorization mechanism it can reveal sensitive information
Open Issues (1/3):
Is Dialog Package Usable for This?

- Dialog package support exists
- Interpretations differ in how they may implement the negative case: “4xx vs empty NOTIFY”
- Only for INVITE-initiated dialogs

- If we don't re-use the dialog event package
  - we need to find some other widely-deployed and well-defined UA behavior that we can leverage
  - or we need to define new behavior on both the caller and callee equipment
    - new method for call-back validation?

Open Issues (2/3): B2BUA traversal

• There is no normative reference in B2BUA behavior we can lean upon and which would be guaranteed to travel end-to-end

• Possible solutions:
  – “if you break it, you fix it” (if you are lucky to be on the reverse path)
  – start working on a token that normatively survives B2BUA traversal
    • draft-kaplan-sip-session-id


IETF73
Open Issues (3/3):
PSTN interworking

- SIP URIs (even with telephone numbers) verifiable with the originating domain using DERIVE
- Unlike TEL URIs which are not clearly associated with an owner

- Do you think it makes sense to attack the TEL URIs?
WG Survey

• Who thinks that life is good without a light-weight way to verify a SIP URI? (and who thinks it isn’t?)

• If folks see the problem, who thinks that reverse URI checking can help to solve it? (not necessarily based on the dialog-package)

• And out of those who would actually like to contribute to this?
BACKUP
A proposed solution

- Use SIP to ask the caller as claimed in From URI “are you calling me”?

alice@atlanta.com  atlanta.com  biloxi.com  bob@biloxi.com

Call

Call

Call

Are you calling me?

Are you calling me?

Yes

Yes

Ring

Ring

Ring
A Proposed Solution (cont.)

- A subscription to the Dialog event package is used to check if the UA registered at the AOR in the “From” header is aware of the call.

- The subscription is restricted to the “half-dialog” formed by Call-ID and From-tag from the INVITE.

- For this, a SUBSCRIBE message is sent to the AOR in the “From” header field from the original INVITE.

- Depending on the result of the subscription, we conclude that the “From” was legitimate, or that we do not know exactly.

- Assumptions:
  - The Location Service at atlanta.com (caller’s domain) is somehow trustworthy
  - Alice is currently registered at atlanta.com
  - IP routing and DNS are not compromised
A Proposed Solution (cont.)

Provisional responses are omitted from the illustration for the sake of clarity.
Related work

• Return routability check:
  – draft-wing-sip-e164-rrc

• Identity:
  – RFC 4474, RFC 3325, RFC 3893, RFC 4916
  – draft-ietf-sipping-update-pai
  – draft-elwell-sip-identity-handling-ua
  – draft-elwell-sip-e2e-identity-important
  – draft-york-sip-visual-identifier-trusted-identity
  – draft-ietf-sip-privacy
  – draft-kaplan-sip-asserter-identity

• Issues with e164 URIs:
  – draft-elwell-sip-e164-problem-statement

• Identity / security on the media path:
  – draft-fischer-sip-e2e-sec-media (expired)
  – draft-wing-sip-identity-media (expired)

... And many others