STIR Charter (discussion)

STIR BoF

Berlin, DE

7/30/2013

For reference

- This is a snapshot of the 7/23 charter version
- Obviously this does not capture any discussion today
- No need to excessively wordsmith here
- This is available on the STIR list for your perusal
- Chairs will ask for hums later, but now let's chat

Preamble

- Over the last decade, a growing set of problems have resulted from the lack of security mechanisms for attesting the origins of real-time communications. As with email, the claimed source identity of a SIP request is not verified, and this permits unauthorized use of source identities as part of deceptive and coercive activities, such as robocalling (bulk unsolicited commercial communications), vishing (voicemail hacking, and impersonating banks) and swatting (impersonating callers to emergency services to stimulate unwarranted large scale law enforcement deployments). This working group will define a deployable mechanism that verifies the authorization of the calling party to use a particular telephone number.

Postamble

- SIP is one of the main VoIP technologies used by parties that want to present an incorrect origin, in this context an origin telephone number. Several previous efforts have tried to secure the origins of SIP communications, including RFC 3325, RFC 4474, and the VIPR working group. To date, however, true validation of the source of SIP calls has not seen any appreciable deployment. Several factors contributed to this lack of success, including: failure of the problem to be seen as critical at the time; lack of any technical means of producing a proof of authority over telephone numbers; misalignment of the mechanisms proposed by RFC 4474 with the complex deployment environment that has emerged for SIP; lack of end-to-end SIP session establishment; and inherent operational problems with a transitive trust model. To make deployment of this solution more likely, consideration must be given to latency, real-time performance, computational overhead, and administrative overhead for the legitimate call source and all verifiers.

The plan (wall o' text)

- As its first work item, the working group will specify a SIP header-based authorization mechanism to verify the originator of a SIP session is authorized to use the claimed source telephone number, where the session is established with SIP end to end. This is called an in-band mechanism. The mechanism will use a canonical telephone number representation specified by the working group, including any mappings that might be needed between the SIP header fields and the canonical telephone number representation. The working group will consider choices for protecting identity information and credentials used, but will likely be based on a digital signature mechanism that covers a set of information in the SIP header fields, and verification will employ a credential that contains the public key and is associated with the one or more telephone numbers. In order to be authoritative, credentials used with this mechanism will be derived from existing telephone number assignment and delegation models. That is, when a telephone number or range of telephone numbers is delegated to an entity, relevant credentials will be generated (or modified) to reflect such delegation. The mechanism must allow a telephone number holder to further delegate and revoke use of a telephone number without compromising the global delegation scheme.

Limitations and Warranties

- The mechanism must allow parties who are not delegated a telephone number, but are authorized by the entity who is delegated the number, to place calls using the identity.

- After completing the in-band mechanism, the working group will consider session establishment where there are one or more non-SIP hops, most likely using an out-of-band authorization mechanism. However, the in-band and the out-of-band mechanisms should share as much in common as possible, especially the credentials.

- Expansion of the authorization mechanism to identities using the user@domain form is deferred since the main focus of the working group is to develop a solution for telephone numbers.

Disclaimers and Pleasantries

- The working group will coordinate with the Security Area on credential management.

- The working group will coordinate with other working groups in the RAI Area regarding signaling through existing deployments.

- Authentication and authorization of identity is closely linked to privacy, and these security features frequently come at the cost of privacy. This working group is not chartered to mandate the presence of identity in SIP requests, and to the extent feasible it will find privacy-friendly solutions that leak minimal information about calls to third parties.

Inputs (won't be in the charter)

- Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks (RFC 3325)
- Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP) (RFC 4474)
- Secure Call Origin Identification
  http://tools.ietf.org/html/draft-cooper-iab-secure-origin-00
- Secure Origin Identification: Problem Statement, Requirements, and Roadmap
  http://tools.ietf.org/html/draft-peterson-secure-origin-ps-00
- Authenticated Identity Management in the Session Initiation Protocol (SIP)
  http://tools.ietf.org/html/draft-jennings-dispatch-rfc4474bis-00

Outputs

- The working group will deliver the following:

- A problem statement detailing the deployment environment and situation that motivate work on secure telephone identity

- A mechanism document describing the SIP end-to-end with telephone number-based identities

- A document describing the credentials required to support telephone number identity authentication

- A fallback mechanism to allow out-of-band identity establishment during call setup

Milestones

- Sep 2013 Submit problem statement for Informational
- Nov 2013 Submit in-band mechanism for Proposed Standard
- Feb 2014 Submit credential specification for Proposed Standard
- Jun 2014 Submit fallback for Proposed Standard