S3-000576

SIP Work in Progress
Some Security Related Aspects

Colin Blanchard BT

Overview

- This contribution is based on some work carried out in BT on how SIP may be used for Service Control in 3GPP. It highlights the following issues, which may impact on the security features for SIP under consideration by 3GPP SA3
  - Call State
  - Call termination

Call State

- Call State is effectively the knowledge that a call is in existence. and is required in some form, to allow service control elements the ability to maintain control over existing calls.

SIP as stateless protocol

- In the true protocol sense, SIP is a stateless protocol.
  - Following the set-up phase of a session, all state is lost. SIP proxy within the CSCF will cease to maintain established Call State and will effectively 'forget' about calls in progress.
- Issue in the context of maintaining existing call ‘usage’ approaches to current telephony charging models call statistics, legal intercept and general maintenance.

Proposed solutions

- There are several possible options for state management.
  - A SIP server can be configured to maintain state (Record Route)
  - User agent state awareness can be utilised for the purpose of service control using Distributed Call State (DCS) procedures
  - Other entities (such a billing engines or application servers) can act as a 'virtual call state machine'.

IETF Work in Progress

- Distributed Call State -
  - The DCS SIP extension proposal suggests that the storage of all state information should be distributed to the clients and suggests a mechanism whereby the Proxy encrypts and signs the state information for endpoint storage [1] [2]
- SIP Servlets -
  - allows a SIP server to defer some of its decision making regarding how to handle SIP request and responses to SIP 'servlets' [6]
- SIP CGI
  - supports a persistence model, which allows state to be maintained by allowing the script to pass a 'token' to the server. When the script is recalled for the same transaction the token is passed back to the script. [5]

BT

SIP DCS

- An extension to the (SIP) that enables proxies to distribute call state to useragents. By providing the ability to distribute state to the user agents where it can be securely stored, proxy servers can remain stateless for the duration of the call. Allows proxies to encapsulate any state information they desire into a header, called a State header, that is delivered to the user agents for a call.

DCS Security

- If the clients/endpoints are considered untrusted entities, the proxy must encrypt the State header and include an integrity check with the State header information. In addition, the proxy is responsible for verifying the contents and integrity of the State header returned by the client

SIP Servlets

- SIP Servlets - A Java extension API for SIP servers. Java code that interacts with a SIP server to control of influence call processing. The server communicates to the servlet by passing objects representing SIP messages.

SIP CGI

- SIP CGI - Can communicate the content of all headers in a SIP request as well as creating all parts of a response, including headers and message bodies. Upon a SIP request the server will pass the body of the message to the script and set up environment variables containing the information on the message headers.

CPL

- Call Processing Language (CPL) - A very simple XML based language that can be used to describe and control Internet telephony services. CPL is designed to be easily created and edited by graphical tools and as it is XML based it is easily parsed. Should be safe as a scripting language as it doesn't permit loops, just conditional statements.[4]

Call State - Conclusion

- Is this an Issue for 3GPP SA3
- If so, the optimum solution may lie in a hybrid model of the ones already proposed by the IETF or perhaps a new proposal may be necessary to better suit the specific requirements of 3GPP.

Call Termination

- It is paramount that the proxy is informed when the session is terminated. There are a number of methods to do this:
  - BYE message
  - Record-Route Header
  - Session timer [3]

BYE Message

- BYE Message - If the INVITE request contained a contact header, the callee SHOULD send a BYE request to that address rather than the From address.
- Can the bye messages be guaranteed to arrive at the proxy
- Could a rogue terminal send bye messages to the proxy, but keep a session alive, thus causing fraud concerns. ?

Record-Route Header

- This header can be added to a SIP Message by any element (i.e. SIP Proxy) that wishes to remain in the messaging chain. This relies on the integrity of the client and is currently not strictly enforceable

Call Termination - Conclusion

- Both the record route and session timer solutions are not strictly enforceable so a desirable solution may come from further examination of (secure) DCS solutions
- Is this an issue with 3GPP.

References

- [1] SIP Extensions for supporting DCS - draft-dcsgroup-sip-state-01.txt
- [2] SIP proxy to proxy extensions for supporting DCS - Draft-dcsgroup-sip-proxy-proxy-01.txt
- [3] SIP Session Timer - Draft-ietf-sip-session-timer-01.txt
- [4] CPL : A Language for User Control of Internet Telephony Services - draft -ietf-iptel-cpl-01.txt
- [5] Common Gateway Interface for SIP - draft-lennox-sip-04.txt
- [6] The SIP Servlet API - draft-kristensen-sip-servlet-00.txt