XEP-0139: Security SIG

Peter Saint-Andre
mailto:xsf@stpeter.im
xmpp:peter@jabber.org
http://stpeter.im/

Will Kamishlian
mailto:will@will-k.com
xmpp:will@jabberdoc.org

2004-09-15
Version 0.2

Status	Type	Short Name
Retracted	SIG Formation	N/A

This document proposes the formation of a Special Interest Group devoted to the analysis of security threats related to Jabber technologies.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

Because security is a core value within the Jabber community, it is appropriate for the XMPP Standards Foundation to assess potential security threats related to technologies that implement the Jabber protocols (including XMPP and defined XMPP extensions), as well as ways to address the threats (for general information about the Internet threat model, see RFC 3552 [1]). Furthermore, since security threats are wide-ranging and of broad concern, it would be valuable for interested members of the entire Jabber community to discuss these matters. Unfortunately, security discussions can often be theoretical, contentious, and inconclusive. Thus it is imperative that discussion proceed based on a methodical process of threat identification, risk analysis, and prioritization before moving on to documentation of threat responses (preferably in protocol specifications such as XMPP Extension Protocols (XEP-0001) [2]). This document proposes a forum and process for such security discussions in the form of a Special Interest Group (see Special Interest Groups (XEP-0002) [3]) that shall report to the XMPP Council [4] in accordance with Article VIII of the XSF Bylaws [5].

2 Scope and Role

The role of the Security SIG shall be to identify and describe security threats related to Jabber technologies, analyze their potential risk, assign priorities to each threat, provide references to existing responses, and (where appropriate) provisionally recommend improvements in Jabber protocols and technologies in order to address the identified threats. The Security SIG shall not itself develop or approve protocols, which tasks shall remain under the purview of the Standards SIG [6] and the Jabber Council respectively.

3 Membership

The Security SIG shall be open to the public and shall not be limited to elected members of the XMPP Standards Foundation. Security SIG discussions shall be conducted in open forums, including a dedicated mailing list at <security-jig@jabber.org>. The process for moderating

[1] RFC 3552: Guidelines for Writing RFC Text on Security Considerations <http://tools.ietf.org/html/rfc3552>.

[2] XEP-0001: XMPP Extension Protocols <https://xmpp.org/extensions/xep-0001.html>.

[3] XEP-0002: Special Interest Groups <https://xmpp.org/extensions/xep-0002.html>.

[4] The XMPP Council is a technical steering committee, authorized by the XSF Board of Directors and elected by XSF members, that approves of new XMPP Extensions Protocols and oversees the XSF's standards process. For further information, see <https://xmpp.org/about/xmpp-standards-foundation#council>.

[5] The Bylaws of the XMPP Standards Foundation (XSF) define the legal basis and operating procedures of the XSF. For further information, see <https://xmpp.org/about/xsf/bylaws>.

[6] The Standards SIG is a standing Special Interest Group devoted to development of XMPP Extension Protocols. The discussion list of the Standards SIG is the primary venue for discussion of XMPP protocol extensions, as well as for announcements by the XMPP Extensions Editor and XMPP Registrar. To subscribe to the list or view the list archives, visit <https://mail.jabber.org/mailman/listinfo/standards/>.

such discussions shall be decided by the members of the Security SIG, but such moderation is strongly encouraged in order to follow the orderly process of threat identification and risk analysis outlined below.

4 Lifetime

The Security SIG shall be a standing SIG, and shall exist as long as the Jabber Council deems it useful.

5 Deliverables

The Security SIG shall produce at least the following deliverables:

1. A brief document specifying the process by which the SIG shall identify, define, analyze, and prioritize a collection of documented security-related threats. This process document will not identify threats or define ways to address them, but instead specify the process to be followed in Steps 2 and 3 below. In defining the process, the SIG should also describe some of its guiding principles, such as:

   a) Rough consensus and running code are superior to ”perfect” solutions
   b) Security measures that cannot or will not be implemented are useless
   c) Iteration works better than trying to define all solutions up front

2. A template to be used for documenting each identified threat. This template should include:

   a) A name for the threat
   b) An abstract that briefly describes the threat
   c) A clear and thorough definition of the threat, preferably to include an attack tree [7]
   d) The estimated likelihood of the threat (e.g., high/medium/low)
   e) The estimated potential damage the threat could cause (e.g., high/medium/low)
   f) A resulting priority for addressing the threat
   g) Existing approaches for addressing the threat (e.g., as documented in a XEP)
   h) The gap between the identified threat and existing responses

[7] For information about attack trees, refer to <http://www.schneier.com/paper-attacktrees-ddj-ft.html>.

i) Potential approaches to addressing the threat or closing the gap, including implementation issues associated with each approach (since security measures that cannot or will not be implemented are useless)

j) Current recommended approach (which may be ”do nothing at this time”)

The template will not fully define the foregoing information, but instead specify what information must be defined for each threat when completing the analysis described in Step 3.

3. An evolving document that completes the template defined in Step 2 for all identified threats by following the process established in Step 1. The result will be a thorough analysis of all potential security threats related to Jabber protocols and technologies. Note: This document shall not define complete solutions to the identified threats, although it may outline potential and recommended approaches. Solutions shall be defined in standalone documents such as XEPs.