# Changes to UCR 2008, Change 1, Section 5.7, Instant Messaging, Chat, and Presence/Awareness

| SECTION | CORRECTION | EFFECTIVE DATE |
|---|---|---|
| 5.7.4 | In the last sentence of the third paragraph, “sensitive information” was changed to “classified and Personally Identifiable Information (PII)” for clarity. | Immediately |

# TABLE OF CONTENTS

**SECTION** **PAGE**

# LIST OF FIGURES

# LIST OF TABLES

# 5.7 INSTANT MESSAGING, CHAT, AND PRESENCE/AWARENESS

## 5.7.1 Introduction

The IM, Chat, and Presence/Awareness features and capabilities listed in this section are not required for all products on the APL, but may be offered as a part of a UC offering. This section begins with a brief overview of IM, Chat, and Presence/Awareness. This is followed by the presentation of the DISR standards for IM, Chat, and Presence/Awareness. The DISR standards are followed by a discussion of the Instant Messaging STIG and the Personal Computer Communications Client (Voice/Video/Collaboration) STIG. The final portion presents the UCR 2008 specific IA requirements.

## 5.7.2 Overview of IM, Chat, and Presence/Awareness

Instant Messaging and Chat provide near-real-time interaction among two or more users. Instant Messaging provides the capability for users to exchange one-to-one, ad hoc text message over an IP network in near real time. Instant Messaging is always user generated and user initiated. Chat, on the other hand, provides the capability for two or more users to exchange text messages in near real time. Chat focuses on group chat or room-based chat. Typically, room persistence is a key feature of multiuser chat. Presence/Awareness is a status indicator that conveys ability and willingness of one user to communicate with other users.

Instant Messaging, Chat, and Presence/Awareness are functions or services that are provided by software products. They are the application programs that create sessions and provide the services. Clients and servers are the computers that execute the application software. Users are the human beings who control the operation of the application programs running on clients. Users are also known as nodes. Each user has a unique username. Each username, in turn, is associated with one and only one server. This server is called the user’s home server.

## 5.7.3 DISR IM, Chat, and Presence/Awareness Standards

The DISR standards provide the basic standards and requirements for DoD implementations of IM, Chat, and Presence/Awareness. The DISR-mandated standard for IM, Chat, and Presence/Awareness is Extensible Messaging and Presence Protocol (XMPP). The core XMPP protocol is defined by RFCs 3920 and 3921. These are being updated. RFC 3920bis-08 and RFC 3921bis-07 are expected to be adopted in the fall of 2009.

As of the publication of this document, the following standards and extensions apply to IM and Chat and are contained in the Messaging & Presence Family section of the DISR:

- RFC 3920: XMPP Core

- RFC 3921: XMPP IM
- XEP-0030: Service Discovery
- XEP-0004: Data Forms
- XEP-0016: Privacy Lists
- XEP-0033: Extended Stanza Addressing (ESA)
- XEP-0071: XHTML-IM
- XEP-0077: In-Band Registration
- XEP-0045: Multi-User Chat
- XEP-0068: Field Standardization for Data Forms
- XEP-0082: Jabber Date and Time Profiles
- XEP-0128: Service Discovery Extensions
- XEP-0115: Entity Capabilities
- XEP-0138: Stream Compression
- RFC 4422: Simple Authentication and Security Layer (SASL) Authentication
- XEP-0191: Simple Communications Blocking

Table 5.7.3-1, Required and Conditional Standards for IM, Chat, and Presence/Awareness, presents a summary of the standards that are required and conditional in accordance with the DISR.

**Table 5.7.3-1. Required and Conditional Standards for IM, Chat, and Presence/Awareness**

| IETF STANDARD | IM CLIENT | IM SERVER | CHAT CLIENT | CHAT SERVER | PRESENCE/ AWARENESS |
|---|---|---|---|---|---|
| RFC 3920: XMPP Core | R | R | R | R | R |
| RFC 3921: XMPP IM | R | R | R | R | R |
| XEP-0030: Service Discovery | R | R | R | R | C |
| XEP-0004: Data Forms | | | R | R | |
| XEP-0016: Privacy Lists | C | C | C | C | |
| XEP-0033: Extended Stanza Addressing (ESA) | C | C | C | C | |
| XEP-0071: XHTML-IM | C | | C | | |
| XEP-0077: In-Band Registration | R | R | R | R | |
| XEP-0045: Multi-User Chat | N/A | N/A | R | R | N/A |
| XEP-0068: Field Standardization for Data Forms | | | R | R | |
| XEP-0082: Jabber Date and Time Profiles | | | R | R | |
| XEP-0128: Service Discovery Extensions | | | R | R | |
| XEP-0115: Entity Capabilities | C | | C | | |
| XEP-0138: Stream Compression | C | C | C | C | C |

| IETF STANDARD | IM CLIENT | IM SERVER | CHAT CLIENT | CHAT SERVER | PRESENCE/ AWARENESS |
|---|---|---|---|---|---|
| RFC 4422: Simple Authentication and Security Layer (SASL) Authentication | | C | | C | |
| XEP-0191: Simple Communications Blocking | | C | | C | |
| XEP-0211: XMPP Basic Client 2008 | R | N/A | R | N/A | R |
| XEP-0212: XMPP Basic Server 2008 | N/A | R | N/A | R | R |

## 5.7.4 STIG Requirements for IM, Chat, and Presence/Awareness

The DISR provides the general standards and requirements. The STIGs provide a detailed set of principles, guidelines, and requirements that serve as the basis for establishing IM systems within the DoD. Instant Messaging, Chat, and Presence/Awareness systems are addressed specifically in the following two STIGs: DISA Field Security Operations, “DoD Instant Messaging Security Technical Implementation Guide,” and DISA Field Security Operations, “DoD Personal Computer Communications Client (Voice/Video/Collaboration Security Technical Implementation Guide.”

In addition to the STIGs, DISA’s Field Security Operations produce checklists that are used as tools to evaluate a system’s compliance with principles and guidelines presented in the STIGs. The checklists for the IM STIGs are the “Instant Messaging Checklist” and the “Personal Computer Communications Client (Voice/Video/Collaboration) Checklist.”

The STIGs and checklists have a broad scope and present very specific requirements for a system’s hardware, software, implementation, operation, and maintenance. The intent of the STIGs is to address all security considerations. The goal is to define processes and procedures, that when applied, will decrease the risk of unauthorized disclosure of classified and Personally Identifiable Information (PII).

## 5.7.5 XMPP UCR 2008 Requirements

### *5.7.5.1 Introduction*

The DISR standards and the STIGs are incorporated into the UCR document by reference. To every possible extent, requirements specified in RFCs and in STIGs will not be repeated in this document. Although every attempt has been made to avoid overlap, some repetition is required to present a logical discussion.

The UCR 2008 requirements are primarily intended to clarify STIG requirements by adding additional detail. The UCR requirements focus on ensuring the confidentiality and integrity of the data as it travels between the XMPP client and the XMPP server, and between XMPP servers. In some instances, the UCR requirements are not consistent with RFC specifications. When differences occur, the UCR specifications shall apply. In all instances, the UCR requirements should be consistent with the STIGs. If any conflicts are observed, the STIG specifications shall apply.

### *5.7.5.2 Concept of Operation*

A user must have a registered account to use the services of an IM, Chat, and Presence/ Awareness system. When the account is established, the user is assigned a unique username. The user is also assigned to one and only one server. This server is referred to as the user's home server. The server's name is a FQDN. Figure 5.7.5.2-1, XMPP Topology, presents a sample XMPP topology. Figure 5.7.5.2-2, Routing of XMPP Messages, presents XMPP routing.

The following presents a high-level overview of the initiation of a client to server XMPP session. This will be followed by the specific requirements for the client-to-server and the server-to-server sessions.

1. The user instructs the client to initiate a session with the user's home server.

2. The client contacts a DNS server and obtains the IP address for the server.

3. The client requests an XMPP session with an encrypted link.

4. The server provides a PKI certificate.

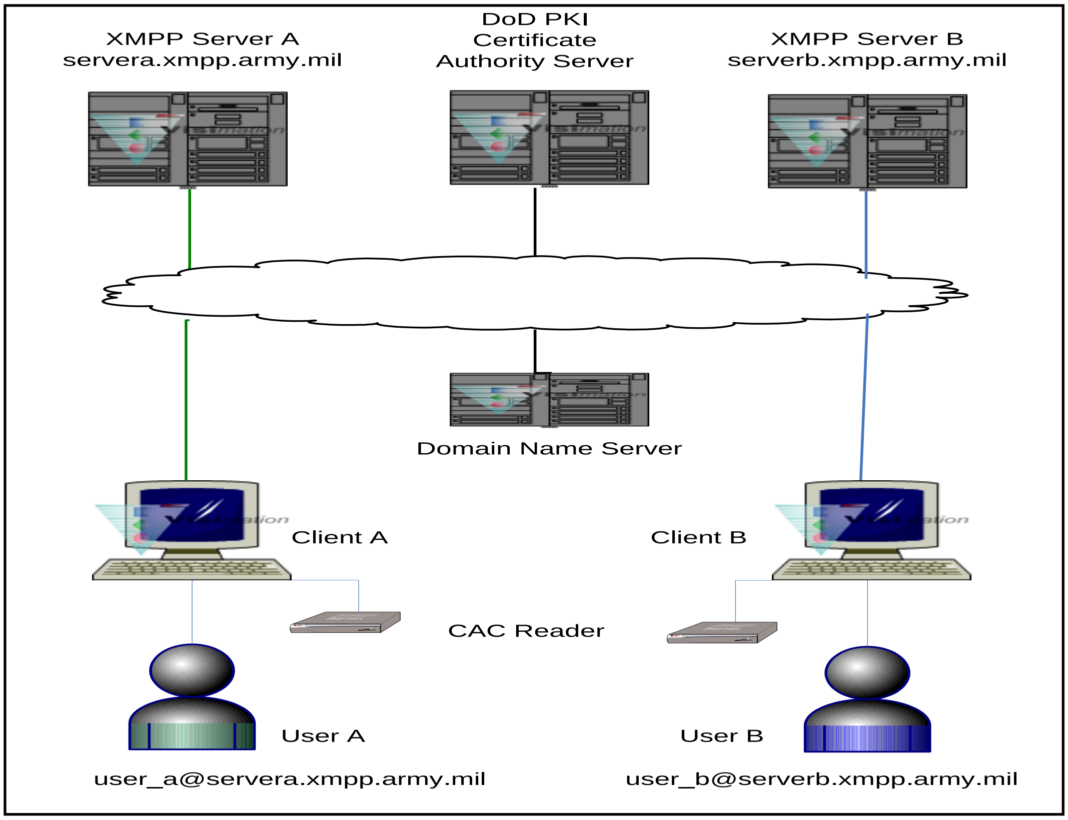

Figure 5.7.5.2-1. XMPP Topology

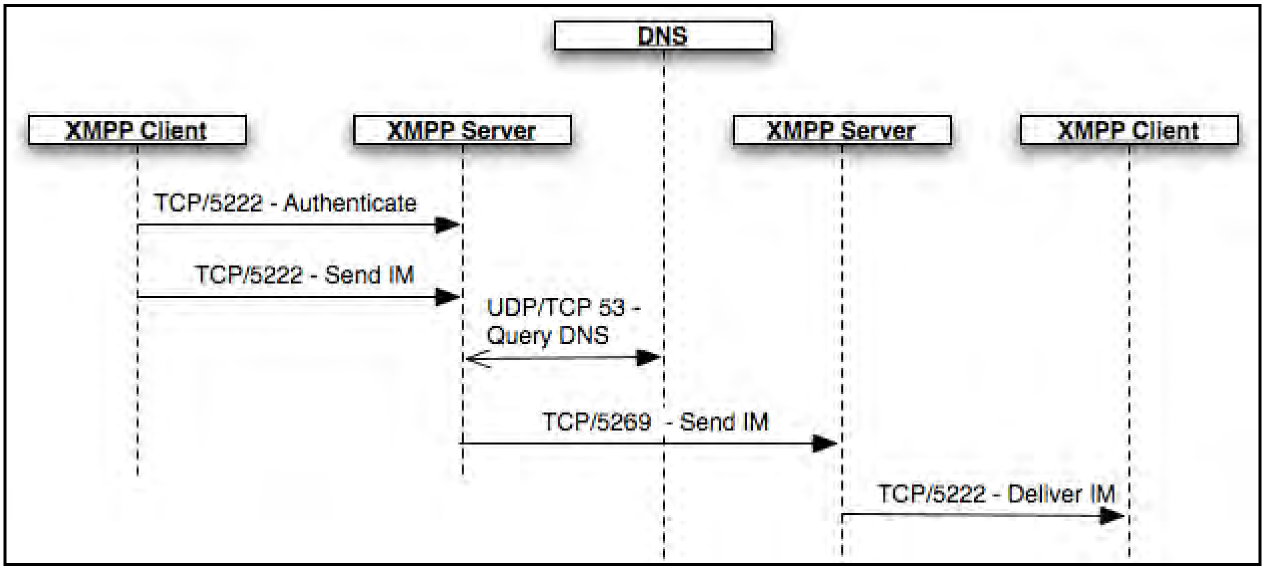

Figure 5.7.5.2-2. Routing of XMPP Messages

5. The client provides a PKI certificate.

6. The server verifies that the provided certificate has not been revoked.

7. The client verifies that the server's certificate has not been revoked.

8. An encrypted TLS session is established.

9. The client authenticates the server.

10. The server authenticates the user.

11. The user begins using the available XMPP services.

### *5.7.5.3 XMPP IA Requirements*

#### *5.7.5.3.1 XMPP General Requirements*

**[Required]** The XMPP clients and servers shall comply with the RFC and RFC extensions listed in Table 5.7.3-1, Required and Conditional Standards for IM, Chat, and Presence/Awareness.

**[Required]** The XMPP clients and servers shall comply with the "DoD Instant Messaging Security Technical Implementation Guide," and with the "DoD Personal Computer Communications Client (Voice/Video/Collaboration Security Technical Implementation Guide," as well as the "Instant Messaging Checklist" and the "Personal Computer Communications Client (Voice/Video/Collaboration) Checklist."

#### *5.7.5.3.2 XMPP RFC and RFC Extension Requirements*

In addition to the RFC and RFC extensions listed in Table 5.7.3-1, Required and Conditional Standards for IM, Chat, and Presence/Awareness, XMPP clients, and servers shall also comply with the following extensions.

**[Required]** XMPP clients shall comply with the XEP-0213 - XMPP Intermediate Client 2008.

**[Required]** XMPP servers shall comply with XEP-0216 - XMPP Intermediate IM Server 2008.

#### *5.7.5.3.3 XMPP User and Server Naming Requirements*

**[Required]** Each user shall be assigned a DoD-wide unique XMPP username.

**[Required]** Each XMPP server shall be capable of being configured with a DoD-wide unique hostname that shall be a FQDN in the ".mil" domain.

**[Required]** Each XMPP server shall have a DoD PKI certificate and the server's host name shall be the Common Name on the PKI certificate.

NOTE: The intent is that the exact same name will be used for the server's host name, the server's DNS name, and the server's Common Name. The MILDEP processes for issuing server certificates were reviewed and this appears to be a standard practice. A similar approach may be used with clients.

### *5.7.5.3.4 XMPP Session Requirements*

**[Required]** The system shall ensure that a user shall only initiate an XMPP session with the user's home server.

**[Required]** When a client initiates an XMPP session with the user's home server, the client shall use TCP/IP port 5222 as the destination port.

**[Required]** All client-to-server XMPP IP packets shall be treated as data packets and shall use the DSCP default bit pattern of 000000.

**[Required]** When a client initiates an XMPP session with the user's home server, the client shall perform a new DNS lookup and use the home server's IP address obtained from the DNS. The client shall not use a configured IP address or a cached IP address learned from a previous DNS lookup.

**[Required]** An XMPP server shall be capable of being configured with a list of the host names of trusted XMPP servers and shall only initiate an XMPP session with an XMPP server that is on the list.

**[Required]** When an XMPP server initiates an XMPP session with another XMPP server, the server shall use TCP/IP port 5269 as the destination port.

**[Required]** All server-to-server XMPP IP packets shall use the DSCP default bit pattern of 000000.

**[Required]** When an XMPP server initiates an XMPP session with another XMPP server, the server shall perform a new DNS lookup to obtain the other XMPP server's IP address. The server shall not use a configured IP address or a cached IP address learned from a previous DNS lookup.

### *5.7.5.3.5 XMPP TLS Requirements*

**[Required]** All client-to-server XMPP sessions shall begin with the establishment of an encrypted TLS session. As defined in RFC 3920, STARTLS is mandatory.

**[Required]** All server-to-server XMPP sessions shall begin with the establishment of an encrypted TLS session. As defined in RFC 3920, STARTLS is mandatory.

**[Required]** If an encrypted TLS session cannot be established, the XMPP session shall be terminated immediately.

**[Required]** DoD PKI Certificates shall be used for all TLS encryption.

**[Conditional]** When a client has a Common Access Card (CAC) reader, the client shall use the certificate on the user's CAC for the TLS session.

**[Conditional]** When a client does not have a CAC reader, the client shall be assigned a DoD PKI certificate and the client shall use its certificate for the TLS session.

**[Required]** The TLS encrypted sessions shall be established in accordance with the specifications presented in UCR 2008, Section 5.4, Information Assurance Requirements.

### *5.7.5.3.6 XMPP Authentication Requirements*

The TLS encrypted session establishes confidentiality. Once this encrypted session has been established, authentication occurs across the encrypted link. Section 2.3 of the Instant Messaging STIG requires IM systems to "link user accounts to directory services (e.g., Active Directory, LDAP) to associate with valid accounts and provide role-based permissions."

**[Required]** Authentication shall occur immediately after the TLS encrypted link has been established.

**[Required]** If authentication fails, the XMPP session shall be terminated immediately.

**[Required]** As part of the authentication, an XMPP client shall authenticate the XMPP server by verifying that the Common Name on the server's DoD PKI certificate is identical to the DNS name of the user's home server.

As part of the authentication, an XMPP server shall authenticate another XMPP server by verifying that the Common Name on the server's DoD PKI certificate is identical to the server's DNS name.

**[Required]** As part of the authentication, an XMPP server shall authenticate an XMPP user by obtaining a password from the user and verifying that the password the user provided is identical to the password stored in the directory service used for authenticating users.

### *5.7.5.3.7 XMPP Future Requirements*

RFC 4622 provides specifications for interfaces between XMPP systems from non-native XMPP user agents and by non-native XMPP applications. As stated in the RFC, providing an interface to XMPP services from non-native applications introduces new security concerns. The ability to interact with XMPP entities via a web browser or other non-native application may expose sensitive information, and thereby, make it possible to launch attacks that are not possible or that are unlikely on a native XMPP network. Because of these risks, support for RFC 4622 is not desired at this time. However, when these risks are fully understood and effective mitigations have been developed, support for interfaces to non-native XMPP applications may become desirable.

RFC 3923 provides specifications for signing and encrypting messages. The specifications only address user-to-user exchanges. Multiuser Chat messages are not included. The RFC requires the use of PKI certificates and requires the user’s XMPP username to be on the certificate. The XMPP user names are not on DoD PKI certificates. However, if DoD XMPP users require the ability to sign and encrypt user-to-user messages, then an extension to the RFC could be developed to provide for an alternate method of authentication. For example, the Common Name on the user’s certificate could be stored in the user’s account information. Therefore, if a need for these features is identified, support for RFC 3923 may become desirable.