

Semantic Chat for Command, Control, and Intel *Beyond Text*

Version 1.0 draft, 2/23/2005

Authors

Michael Behrens, R2AD, LLC

Abstract

Chat tools have been around for a long time and have recently been recognized as a critical communication tool for communicating intelligence and command and control between and amongst organizations and security levels. Chat is also now a de-facto tactical tool. This paper covers a few of the important aspects of the chat utility and proposes how chat content can be enriched with a semantic layer.

This informational document assumes that tags compliant with specifications produced by standard bodies (IETF, OASIS, GGF, etc) and from active working groups such as the Intelligence Community Metadata Working Group [ICMWG] and are being used to ensure that chat protocol can inter-operate and that content can be properly filtered and sanitized.

Status

This white paper is an **initial draft** release and is provided for review and evaluation only to solicit your contributions and suggestions in the near future. This paper will be distributed widely in hopes that it can help stimulate enhancements.

COPYRIGHT NOTICE

© 2005 R2AD, LLC. All rights reserved. No other rights are granted by implication, estoppel or otherwise.

R2AD is a registered trademark of R2AD, LLC in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Permission to copy and display this "Semantic Chat for Command, Control, and Intel" Whitepaper ("this Whitepaper"), in any medium without fee or royalty is hereby granted, provided that you include the following on ALL copies of this Whitepaper, or portions thereof, that you make:

1. A link or URL to this Whitepaper at this location.
2. This Copyright Notice as shown in this Whitepaper.

The information contained in this document represents the current view of R2AD, LLC on the issues discussed as of the date of publication. Because R2AD must respond to changing market conditions, it should not be interpreted to be a commitment on the part of R2AD, and R2AD cannot guarantee the accuracy of any information presented after the date of publication.

R2AD, LLC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

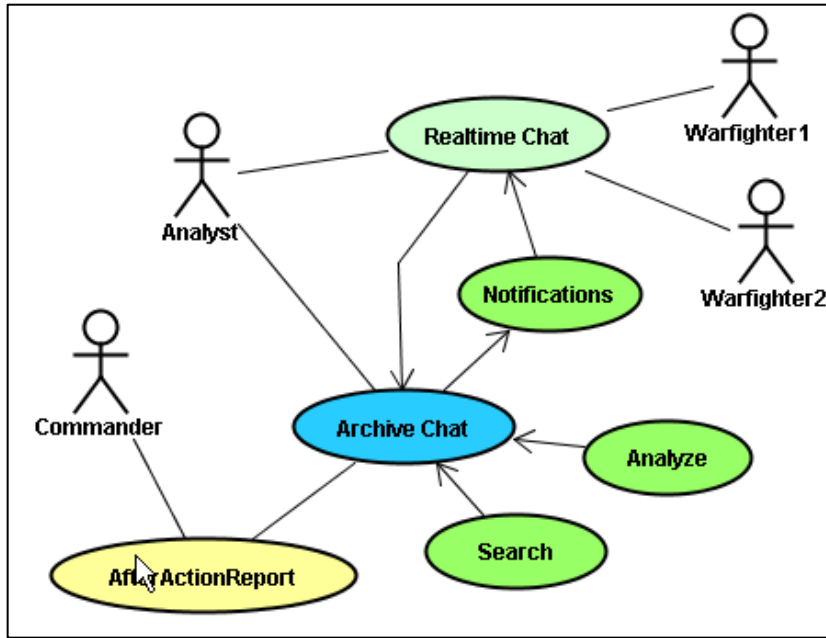
R2AD may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from R2AD, LLC, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). THIS WHITEPAPER IS PROVIDED "AS IS". R2AD, LLC, BiblioTronix, LLC (COLLECTIVELY, THE "COMPANIES") MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THIS WHITEPAPER ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THE COMPANIES WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO ANY USE OR DISTRIBUTION OF THIS WHITEPAPER.

Lets Chat

Currently the core capability of a chat tool is to enable peer2peer or client/server textual communication. Recent enhancements and integration efforts offer capabilities that provide proven military utility in efforts such as Operation Iraqi Freedom (OIF).

What follows is some discussion on a variety of topics which is of interest to those considering developing or integrating chat into mission critical and non-critical applications.



Embedded Semantics – adding objects

If a chat GUI can interpret security tags, the next logical step is to also embedded object tags which can be interpreted by applications on either side to provide information sharing between applications (and hence users). The classical example is that of something on the map. A user drag gesture could place a “reference” to the item in the chat window. When others receive the item an icon and label would be presented, indicating that there is rich content available by dragging the object link to the local application for retrieval and visualization/processing. The link would need to follow standard published specifications for external references, such as WS-Addressing. This powerful capability was originally suggested

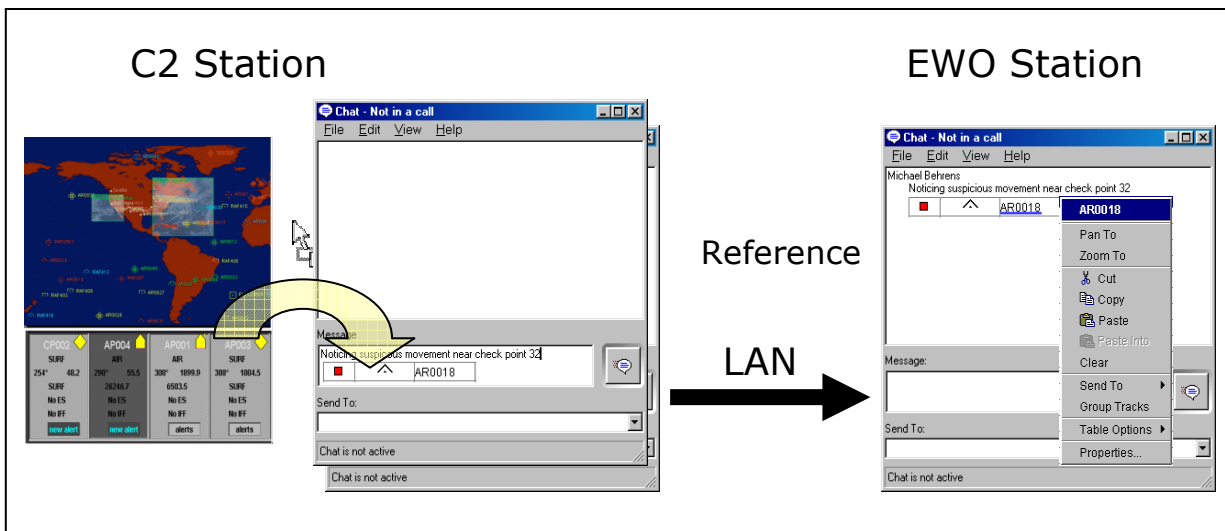


Figure 1 - Drag/Drop to/from Chat

in 2000/2001 via a Polesis brief to DISA as part of a PDR review for the ABA ACTD.

A more specific example would be to embed an alert XML document within the chat content that compliant with the OASIS Common Alerting Protocol [CAP]. This would enable geographic related information to be disseminated and used on the receiving end in a map.

These tags would need to be agreed upon with regard to semantics¹.

Search

Current chat tools being developed and demonstrated as part of pilots and exercises add to the basic chat capabilities and provide persistent store of chat content. This stored content can be a valuable source of information that should be available for outside examination. Search engines and capabilities can then index the chat content and provide rapid access to content at multiple security levels.

From a user perspective, general search attributes would be:

- Time Frame
- Topic
- Unit Name (1/2/D)
- User Name
- User Location (possibly content location)
- Server/chartroom

Google: Installing a Google appliance on the same network as the logging server such that the content could be indexed by Google would provide a basic and powerful capability for the end user. Google also provides web services and APIs that can be exploited by applications.

Tactical Chat (War Fighter)

The distinctive qualities of tactical communication require that the user interfaces are simple and content is usually concise. Input devices might small and would have small screen real estate. Some client side detection of keywords that might help the operator enter information faster is desirable. Audible announcements can also help.

Analyst Chat

Analysts work with full client hardware and good communication lines. They can use multiple chat windows and can monitor tactical chat content. They can use other systems at the same time and can help interpret and augment tactical content.

Server Add-on Processing

Additional server or client side capabilities might include gazetteers that can Geo-Parse the content and perform dictionary lookups to provide auxiliary information such as coordinates for a name.

Language translation is another example of server side functions that could be provided once standards are utilized.

Post Processing

Once chat content is available and searchable, higher order hierarchical organizations can build on the information, disseminate it as reports, mark-up, etc. A story can then be created which would be the result of distilling other information such as imagery. This information would constitute a record set which would be the output of analysis and not the raw chat content.

¹ http://www.bibliotronix.com/publications/whitepapers/SemanticExchangeProtocol_v1-1.pdf

HAL Chat

Sometimes it might be desired to send automated messages from non-humans (machines) over a chat channel. This spawns requirements on the server side to process chat data and injects new messages based on configured rule-sets. Also, alerting or other notification mechanisms could be configured to also support chat rooms so that if need be, one or more persons can be sent a message from outside the chat software via an API provided by the chat server suite.

Furthermore, while chatting is taking place, metadata about the participants can be shared, such as geo-location information which would help folks know where everyone is. Most field devices have GPS embedded in them.

Inter-Chat

Since chat rooms and servers are dispersed geographically, the question must be raised about how users in different locations can chat with each other or search across chat servers (domains). Furthermore, the automated chat injection mechanisms might be useful to help with collaboration across the enterprise.

Data Mining

Many different analytical tools can be applied to the chat data. Chat content might also contain embedded documents (word, images, etc). Dimensional Modeling: A way to model aggregated facts with their supporting data from the data warehousing field. Essentially a post analysis function would be to link chat data with other data so that a dimensional model could exist.

Network Interfaces

For searching chat content, a standard network service is desired. This service would ideally be registered with available NCES discovery services. This service would most likely be implemented as a web-server. On the publishing side, content-staging services might be used.

After Action Reporting

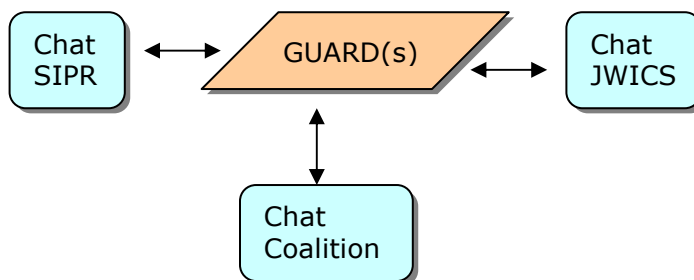
As units come back from a mission (i.e.: recon patrol), their raw chat content and any automated processing (geo-parsing) can be used to review the mission and prepare the report. This process would help to train the war-fighters to use the tools so that the content can be most informative.

Cross Security Domain

Cross-Domain versions add the benefit of being able to exchange textual information between one or more parties on different security levels. There are several versions of "Cross-Domain" or "Multi-Level" chat tools being tested. One approach might be to treat all content from a network to be at one classification and only secondary copy/paste operations between tools would allow cross-domain communication. A more dynamic approach would be to allow tagging within each message to empower the originator to tag sections of data with classification.

Pilots of CDS chat have taken place [Multi-level Chat] within the Intelligence Community (IC-CIO). These pilot tests have shown that users like the added benefit of communication and quickly get used to declaring security levels while using the application.

Ensuring that the users can understand the benefit of tagging the data so that it can contribute to collaboration is important. There is also concern over where the authority lies with declaring content to be at a different security level than the network.



Terminology and Concepts

The following definitions outline the terminology and usage in this paper.

Metadata:

Information about data, generally of the pedigree/providence nature.

Acknowledgements

Some of the concepts described here came from work with DARPA, DISA, and the GCCS-J Integrated Imagery and Intelligence (I³) team. A chat requirements meeting was held 23 November 2004 at Northrop's Philadelphia WestCon office.

References

[Jabber]

<http://www.oasis-open.org/committees/download.php/5531/oasis-200401-wsssoap-message-security-1.0.pdf>

Jabber.com, Jabber.org

[NRL Chat]

NRL, Multilevel Chat, PowerPoint slide, macklint/PJ, Naval Research Laboratory
www.crosstalk.csp.sgov.gov

[Multi-level Chat]

PowerPoint slides, Cross Domain Solutions Working Group (CDSWG), 22 Jan 2004, MITRE, CIA/NSA JPO, mejone1@missi.ncsc.mil

[CrossTalk]

Cross Domain Instant Messaging, IC-CIO CrossTalk, Don Centek, Project Manager, donjc@ucia.gov, CDS-WG Briefing – 8
December 2004

[ICMWG]

Intelligence Community Metadata Working Group
<http://www.xml.saic.com/icml>

[CAP]

OASIS Common Alerting Protocol (CAP)
<http://www.oasis-open.org/committees/download.php/6334/oasis-200402-cap-core-1.0.pdf>
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency