SENTINEL SECURE CHAT - BANDWIDTH SAVINGS

Data Optimization and Compression for Tactical Edge Mission Communications.

https://www.tacticalchat.com/compression-feature/

BLUF: Data Savings, Stated in 3 Different Ways

- **Fact 1: SENTINEL saves 90% of the current bandwidth required by IRC chat clients, 97% of XMPP clients and 99% of Chatsurfer and Element Clients**
- **Fact 2: SENTINEL uses 1/10th the data of IRC clients, 1/37th the data of XMPP clients, 1/58th the data of Element, and 1/78th the data of Chatsurfer**
- **Fact 3: 8 SENTINEL Clients use less data than 1 mIRC or 1 Mako Client, 36 SENTINEL Clients use less data than 1 Transverse Client, 58 SENTINEL Clients use less data than 1 Element Client, 73 SENTINEL Clients use less data that 1 Chatsurfer Client**

SYNOPSIS:

Mission communications for tactical edge units (AWACS, UAS, CAS, and JTACs) are routinely performed in environments, and with equipment, that offer limited bandwidth capacity.

Lab testing demonstrates that SENTINEL Secure Chat systems provide superior data compression routines, saving 90% of the current bandwidth required by other legacy IRC chat clients, 97% of XMPP clients and 99% of Chatsurfer and Element clients.

This brief overview outlines the lab test and findings, the compression capabilities of SENTINEL and considers the mission impact of the SENTINEL Secure Chat compression.

SENSITIVE INFORMATION MAY BE INCLUDED: Please, protect this information and technical data that may be observed by adversary intelligence systems or that may be interpreted or pieced together to derive critical information in time to be useful to adversaries. Protect information and technical data that provides any insight into vulnerabilities of U.S. infrastructure, including DoD warfighting infrastructure that are otherwise not publicly known or available.

BACKGROUND

Chat communications have become critical for the command and control of manned and unmanned missions, providing clear, nearly instantaneous situational awareness of operations among Controllers, Commanders, Senior Leaders, and Approval Authorities – all in disparate locations. Chat continues to grow in use, with many missions requiring the availability of this capability to gain approval for launch or mission execution.

Trusted Solutions has provided secure tactical chat software for customers with no fail missions for over a decade. Our chat servers have been operational with Department of Defense units since 2010, with focused improvements and features remaining in-step with our customers and their missions. These back-end servers have been the backbone for chat communications, reliably routing and logging message traffic in real world operations.

While remaining engaged with our customer requirements, we have also been aware of the need for a DoD accredited and approved solution for the front-end application side of chat communications. In late 2020, Trusted Solutions began developing a DoD focused Tactical Chat Client, merging it with the in-use back-end servers into a single, secure system known as SENTINEL, bringing together the previous functions of legacy chat clients into a reliable, modern, user-friendly interface that reduces the required time for training and familiarization with the software.

Having control of the development and use of both the back-end server and the front-end client application in a chat communications system brought forth multiple mission advantages. One of these advantages is being able to provide increased security and functionality with the interaction of the SENTINEL Server and SENTINEL Client. Increased security features include true end-to-end secure file sending, non-repudiation of all user activity, and the ability to clearly identify all chat users within the system.

Another increase in functionality, and one of the most significant, is with the SENTINEL Server and SENTINEL Client working together as a system. We were able to build a SYSTEM that integrates compression algorithms in the transmissions of text chat and in the secure file sending. Bandwidth constrained units and platforms at the tactical edge can now see a reduction in dropped connections and experience more stable communications based on this improvement with SENTINEL. This paper is intended as a summary of the gains realized when testing these compression capabilities.

SENTINEL DATA HANDLING CAPABILITIES

The introduction of the SENTINEL Chat Client and SENTINEL Server update provides the DoD units and organizations many powerful chat and file sending features while continuing to meet specific DoD and mission requirements. SENTINEL's most important improvement may be its ability to handle and compress data for limited bandwidth networks. These internal processes for data handling and compression are significant and will dramatically and positively affect tactical edge user mission users such as AWACS, Submariner, JTAC, CAS, Riverine, UAS and intelligence gathering missions.

In Mission networking monitoring shows data savings of 90% during transmission over the legacy chat client and server configurations currently utilized by the US DoD and its affiliated nation mission partners. This means that 10 AWACs planes, running a SENTINEL Chat Client, would use less bandwidth than 1 single AWACs plane running a legacy chat client.

DoD CHAT CLIENT DATA USAGE AND COMPARISON TESTING

The US Department of Defense (DoD) currently utilizes various chat client software packages and various chat protocols, including Internet Relay Chat (IRC) and Extensible Message and Presence Protocol (XMPP). To better understand how these various software packages and protocols handle text and data across bandwidth restricted networks, Trusted Solutions compared the most mission utilized chat clients to its SENTINEL Secure Chat solution.

The compared chat client software packages include:

SENTINEL Chat Client (IRC)

SENTINEL Chat Client is a US assured, DoD Only distributed chat solution and developed directly from US military mission user feedback to meet DoD requirements over the last decade.

SENTINEL continues to be supported and developed in step with the ever-changing mission. This client currently operates on the Internet Relay Chat (IRC) protocol to ensure reliable chat communications in bandwidth restricted mission applications. It is compatible with all known IRC servers and can communicate with XMPP users via its companion SENTINEL Chat Server solution.

Mako (IRC)

Mako is an older (+10 years) US NAVY built software platform that uses IRC as its protocol. Mako is at end-of-life, no longer being supported or maintained.

mIRC (IRC)

Not officially sanctioned by the DoD, mIRC is a widely used shareware Internet Relay Chat (IRC) protocol chat client.   It is also used by individuals, such as gamers, software development groups, hackers, and other technically minded organizations to communicate across IRC networks.

Pidgin Chat (XMPP)

Pidgin is an open-source chat program which lets you log into accounts on multiple chat networks simultaneously. The interface is built in Java and lets users can on to XMPP and IRC server channels at the same time.

Transverse Chat (XMPP)

Transverse is an XMPP based software platform also built on Java. Its server experienced a log4j security vulnerability in 2022 and the software develop cancelled support and maintenance of this product. It is also at end-of-life.

Chatsurfer

Chatsurfer is a web-based chat tool. Technically not a client, but more like a web session. It uses the HTTP protocol for data transmission.

Element

Element is an open-source client program running on the Matrix protocol and server.

CHAT CLIENT and SERVER TESTING CONDITIONS

The following method of testing for each of the software packages/configurations was developed to allow for a comparison of each system specifically to SENTINEL Secure Chat. This was an internally conducted and an independently verified test. The testing procedures and measures have been outlined here to allow further independent testing to verify Trusted Solutions' findings.

1. All chat client software solutions are running on the same hardware platform and network, connected to a SENTINEL Chat Server.

2. SENTINEL, Mako and mIRC are connected to the SENTINEL IRC server.

3. Pidgin and Spark and Transverse are connected to the SENTINEL XMPP server

4. All IRC and XMPP clients are connected to the same three (3) rooms/channels via the SENTINEL SERVER GATEWAY

5. Each Channel / Room on the server is running AI bots that simulate chat traffic to the server and to the clients.

6. The data traffic is viewed via a network diagnostic software tool.

7. The data processed and handled by each client is recorded at various intervals in a mission like environment for periods of 40 minutes of operation, 60 minutes of operation, 3 hours in, and after a 12-hour period. 40 minutes and 3 hours are shown in the video.

A video capture of the network test run to collect the values below may be viewed at: https://www.tacticalchat.com/compression-feature/

LABORATORY TEST FINDINGS

The data reported demonstrates:

1. The SENTINEL Chat Client utilizes 1/10th, or 90% less data than other IRC clients.

2. SENTINEL utilizes approximately 1/37th, or 97% less data compared to the XMPP capable clients Pidgin and Transverse.

3. SENTINEL utilizes approximately 1/58th, or 98.3% less data compared to the Element Client.

4. SENTINEL utilizes approximately 1/74th, or 98.6% less data compared to Chatsurfer.

STATS: Same data / same hardware / same network conditions

SENTINEL	lowest data transmitted
mIRC	9.5 times more data than SENTINEL
Mako	9.0 times more data than SENTINEL
Transverse	37.9 times more data than SENTINEL
Pidgin	37.8 times more data than SENTINEL
Chatsurfer	74.0 times more data than SENTINEL
Element	58.7 times more data than SENTINEL

A video capture of the network test run to collect the values below may be viewed at: https://www.tacticalchat.com/compression-feature/

ABOUT TRUSTED SOLUTIONS

Trusted Solutions is a U.S.-based, Veteran's Administration verified Veteran Owned Small Business (VOSB) based in Nashville, Tennessee. The company was founded to fill a need for secure and reliable chat communications for U.S. Department of Defense units and organizations, and our veteran led perspective responsively assists our DoD client's global mission efforts.

Hundreds of missions a day are coordinated on Trusted Solutions' secure chat platform, with warfighters depending on our software's capability, reliability, and no-fail technical support. Our DoD approved technology provides simultaneous IRC and XMPP chat capabilities, and bridges these protocols seamlessly across multiple domains, networks, and communities.

KEY CAPABILITIES:

- Chat Technology Program Level Management (IRC / XMPP / and various platforms).
- Secure Chat Technology Custom Development for Mission applications.
- Our Chat Software is in mission use NOW with proven reliability and results.
- U.S. based company providing the US Government Product and Process Accountability
- Current chat solutions were built as a coordinated effort with U.S. Military, NATO Partners and Information Assurance personnel.
- Engineered to meet current mission and security needs, and flexible to facilitate future and forward-thinking requirements.
- U.S. DOD security cleared personnel.
- U.S. Veteran Engineers developed the current chat networks in use today.
- US only company developed, supported, and assured.
- On-site setup, worldwide. / On-Site, short- and long-term support available.
- Client and server level administrator training available.
- 24/7 Reach Back Support.

STATUS:

US Owned, Certified Service-Disabled Veteran Owned Small Business (SDVOSB)

Technical Development Contact:	**Business / Operations Contact:**
Tony DePasquo	John C. Nalls
tony.depasquo@tacticalchat.com	john.nalls@tacticalchat.com
+1 (615) 975-5625	+1 (571) 400 -8785