SENTINEL SECURE CHAT BANDWIDTH SAVINGS

Data Optimization and Compression for tactical edge mission communications.

SYNOPSIS:

Tactical Edge Mission communications for AWACS, Submariner, JTAC, CAS, UAS, and any Intelligence gathering missions are routinely performed in environments, and with equipment, that offers very limited bandwidth capacity.

It has been demonstrated that SENTINEL Secure Chat systems provide superior text and file sending data routines that save 90% of the current bandwidth required by other existing chat and file sending systems.

This brief overview demonstrates these capabilities and hopes to consider the mission multiplying effects of the SENTINEL Secure Chat Solution and its inherent data optimization and compression routines.

FOR MORE INFORMATION

Trusted Solutions, LLC
Tony DePasquo
tony.depasquo@tacticalchat.com
+1 (615) 975-5625

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.

TABLE OF CONTENTS

BACKGROUND

Since 2007, Trusted Solutions has provided secure tactical chat with continuous mission focused improvements and features at the Air Force's Combined Aviation Operations Center (CAOC) located in Al Udeid, Qatar (AUAB)

During this period, utilizations of mission-based chat at AUAB have grown exponentially from a few hundred users to 3000+ daily mission users, and Trusted Solutions' chat technology reliably connects an average of 26 million Mission Message Exchanges (MME) every month; averaging nearly 300 million Mission Message Exchanges annually. Similar growth of chat usage is common across the entirety of US DoD missions and has become a staple for modern mission success.

To ensure the chat network at the CAOC located at AUAB remain mission capable, while simultaneously meeting Defense Information Security Agency (DISA) requirements for the inclusion of specific XMPP and other Security capabilities (UC XMPP, Jan 2013), several key technical developments are integrated into Trusted Solutions' current Internet Relay Chat (IRC) solution, known as SENTINEL Secure Chat.

SENTINEL DATA HANDLING CAPABILITIES

While the inclusion of the SENTINEL chat client and SENTINEL server updates provides the Air Force with many powerful chat and file sending features and is continuing to meet specific DoD and mission requirements, one of SENTINEL's most important improvements 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.

Our recent lab studies and tests have shown data savings of 90% during transmission over other chat client and server configurations being utilized by the US DoD and its affiliated nation mission partners.

DoD CHAT CLIENT DATA USAGE AND COMPARISON TESTING

Currently, the US Department of Defense (DoD) 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 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 developed in step with 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 know IRC servers and can communicate with XMPP users via its companion SENTINEL Chat Server solution.

mIRC (IRC)

mIRC is a probably the most popular shareware Internet Relay Chat (IRC) protocol chat client used by operational DoD units. However, it is not officially sanctioned by the DoD. It is most 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. This means that users can log on to XMPP and IRC server channels at the same time. Pidgin is compatible with the following chat servers and chat networks: Jabber/XMPP, Bonjour, IRC, Novell GroupWise Messenger, Lotus Sametime, SILC, and Zephyr.

Spark Chat (XMPP)

Spark is an Open Source, cross-platform XMPP and IRC chat client optimized for businesses. It features built-in support for group chat, telephony integration, and strong security. It is often combined with an Openfire XMPP protocol server.

THE TEST CONDITIONS

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

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

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

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

5. Each IRC client type is connected via a secure SSL connection simulating users with SSL requirements

6. A duplicate of each IRC client type is also connected to a non-secure, non-SSL connection simulating many current users on closed networks

7. Each XMPP capable client is connected via a secure SSL connection

8. Each Client Software has the exact same nine (9) channels / rooms

9. Each Channel / Room on the server are running AI bots that simulate chat traffic to the sever and to the clients

10. The data traffic is viewed via two distinct network diagnostic software tools. Using two (2) network diagnostic tools ensures that different tools are reporting the same network traffic for each client software solution. The Network diagnostic software used were as follows:
    a. TCPview Software
    b. CurrPorts Software
    c. Also…Window Task Manager was available

11. The data processed and handled by each client is recorded for periods of initial connects and joins at ~1 minute, 30 minutes, 60 minutes, and 90 minutes. ***See the recorded data below on page 4.***

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

CHAT CLIENT DATA HANDLING LAB TEST FINDINGS

The data reported demonstrates:

1. SENTINEL Chat Client utilized 1/10 or 90% less data than its closest competitor mIRC.

2. SENTINEL utilizes approximately 1/28 or 97% less data compared to the XMPP capable clients Pidgi, Tranverse, or Spark.

BY CONNECTION TYPE	PERIOD OF TIME	BANDWIDTH USED		SENTINEL DATA SAVINGS (30 MINUTES)
NON-SSL CONNECTION				
SENTINEL Non-SSL	30 Minutes	2,526.00	Bytes	N/A
mIRC Non-SSL	30 Minutes	45,471.00	Bytes	94%
SSL CONNECTIONS				
SENTINEL SSL	30 minutes	6,730.00	Bytes	N/A
mIRC SSL	30 minutes	68,107.00	Bytes	90%
XMPP SSL CONNECTION				
Pidgin XMPP SSL	30 Minutes	179,326.00	Bytes	96%
Spark XMPP SSL	30 Minutes	192,926.00	Bytes	97%

BY CONNECTION TYPE	PERIOD OF TIME	BANDWIDTH USED		SENTINEL DATA SAVINGS (90 MINUTES)
NON-SSL CONNECTION				
SENTINEL Non-SSL	90 minutes	122,468.00	Bytes	N/A
mIRC Non-SSL	90 minutes	2,148,821.00	Bytes	96%
SSL CONNECTIONS				
SENTINEL SSL	90 minutes	179,724.00	Bytes	N/A
mIRC SSL	90 minutes	3,212,442.00	Bytes	92%
XMPP SSL CONNECTION				
Pidgin XMPP SSL	90 minutes	8,407,379.00	Bytes	98%
Spark XMPP SSL	90 minutes	8,065,266.00	Bytes	98%

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

With hundreds of missions a day being coordinated on Trusted Solutions' secure chat platform, warfighters have come to depend on our software's capability, reliability, and no-fail technical support. Our veteran led perspective responsively assists our DoD client's global mission efforts. 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 Disabled Veteran Owned Small Business (DVOSB)

Technical Development Contact:

Tony DePasquo
CEO / CTO
tony.depasquo@tacticalchat.com
+1 (615) 975-5625

Business / Operations Contact:

John C. Nalls
COO
john.nalls@tacticalchat.com
+1 (571) 400 -8785