Starburst Multi-Compartment Chat Phase 2

APRIL 2020

Developers: John Coon, Steven Polk, Robert Rasmussen, Michael Lee, Preetham Pamulapati
Coach: Dr. Richard Newman,
Liaison: Mark Sanders

INTRO/PROBLEM STATEMENT

- The current email system in place within Raytheon is too slow to communicate important classified information effectively

SOLUTION

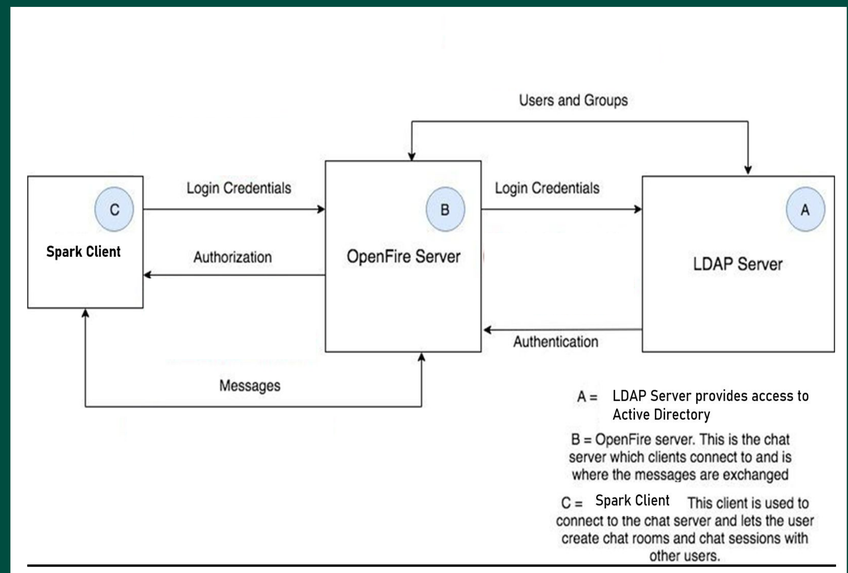
- Replace the current email system for classified and confidential information sharing via a real time chat application that is in compliance with DOD security protocols and directives

METHODS

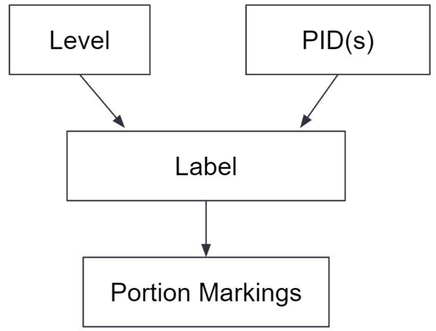
1. The Phase 1 team Transcrypt did research on open-source chat clients and servers. They determined that Spark and Openfire had the security and flexibility needed to accomplish our tasks.
2. Compared opensource and off-the-shelf chat services
3. Researched Spark and Openfire plugins and documentation.
4. Cyclic pattern of research, developing, and testing.
5. Main form of testing was manual, real-time testing.

Main server that Spark connects to, communicates and receives information about certain users from Active Directory

Main User Interface, Users will login with credentials



Important Term Relations:



- Labels - The classification of the chat room
- Levels - sensitivity of user, room, or message
- Program Identifiers (PIDS) - The project(s) the user is cleared for.
- Portion Markings - The label of the message being sent

Standards:

- PL3 (Protection Level 3) - Everyone in environment has top clearance, different need-to-know categories
  - Access control, Auditing, Identification and authentication, Least privilege, Marking
- CAPCO - machine and human readable standard for marking information
- XMPP (eXtensible Messaging and Presence Protocol) - Security Standard applicable to all instant messaging and presence indicator software

Herbert Wertheim College of Engineering
Department of Engineering Education
UNIVERSITY of FLORIDA