
Multilevel Chat (MLChat)

Tom Macklin, Phyllis Jenket
Center for High Assurance Computer Systems
Naval Research Laboratory



- Collaboration in a net-centric environment:
 - Multinational user communities must coordinate operations:
 - In near-real-time <3 seconds
 - Guarantee delivery
 - All users receive same information simultaneously
 - Tactical environments limit resource availability
 - Space, weight, and power
 - User and administrator training
 - Network bandwidth and quality of service



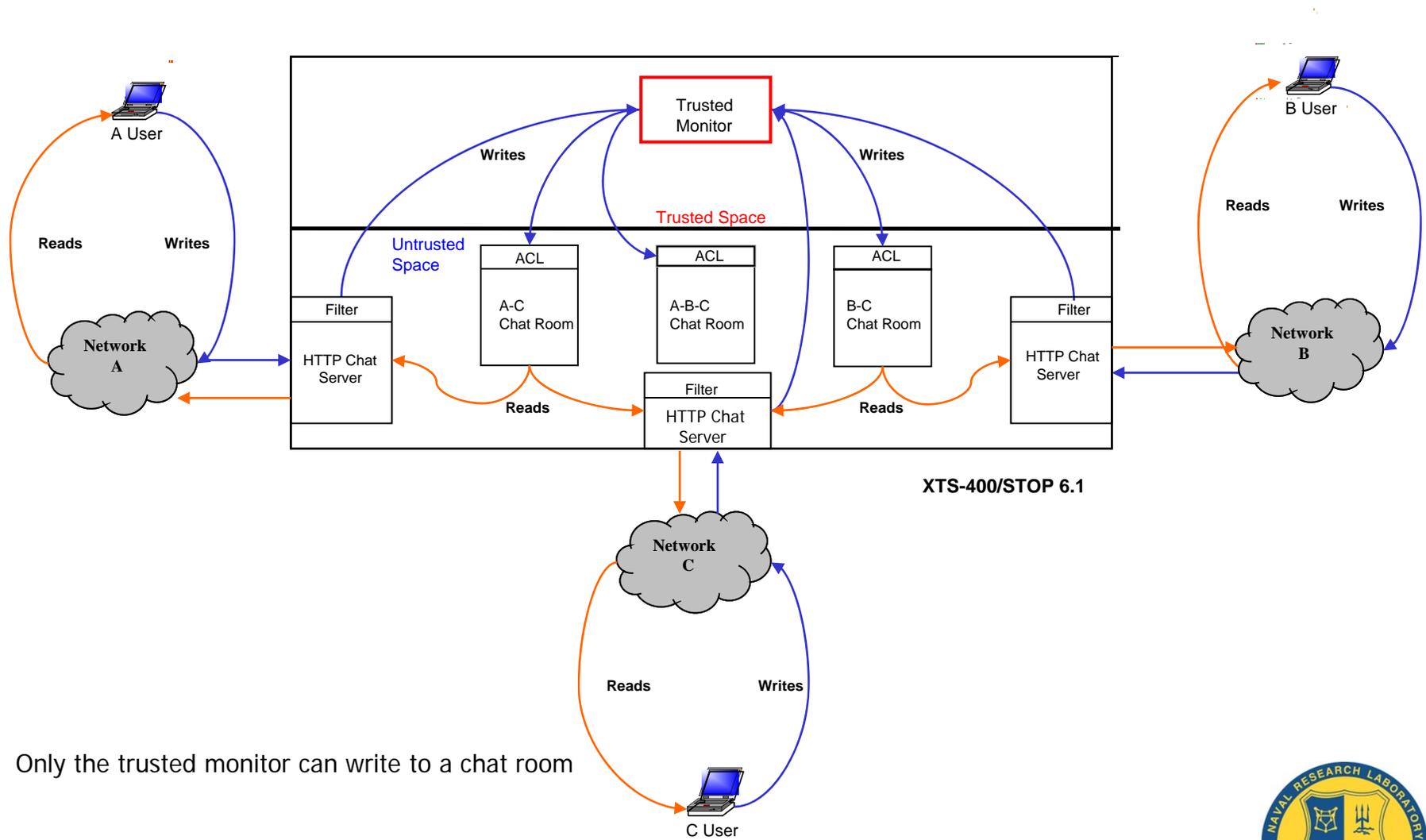
- **MLChat Hybrid Architecture:**
 - Provides chat services on a single multi-level secure (MLS) server
 - Connects MLS chat servers to networks of differing security levels (MSL)
 - Mediates all data writes through a trusted process (Guard)
 - Supports multiple chat rooms that run at specific levels, and allow access based on user, network clearances and permissions



- **Multilevel Chat Critical System Components:**
 - **STOP Operating System Mandatory Access Controls**
 - Strong process separation for different enclaves
 - Chat rooms protected so that only authorized enclaves may access them
 - **Trusted Chat Monitor**
 - Mediates all message exchanges between enclaves
 - Performs message content validation
 - Manages/monitors chat server instances
 - **Chat Server Instances**
 - Commercial-off-the shelf, modified to support labels
 - ASCII character filter
 - Enhanced security for administrative controls
 - MAC protections for chat room access control lists
 - Integrated data labels into chat clients



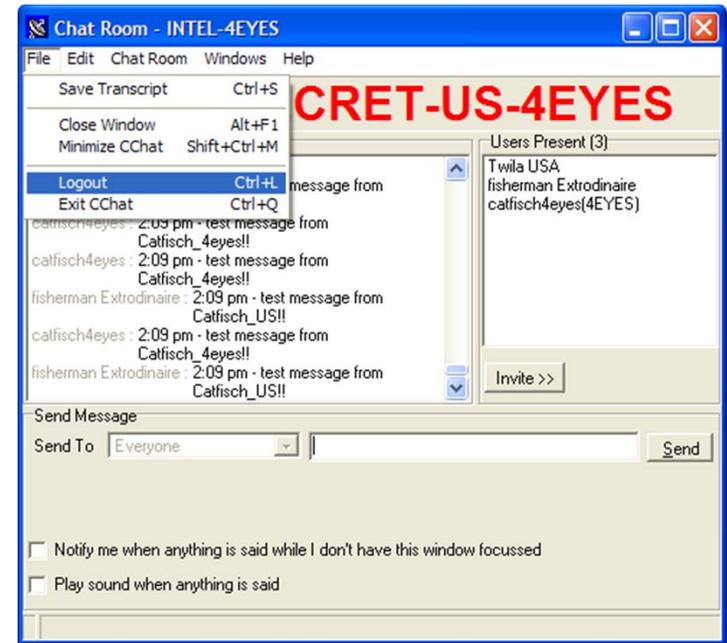
Trusted vs Untrusted Environment



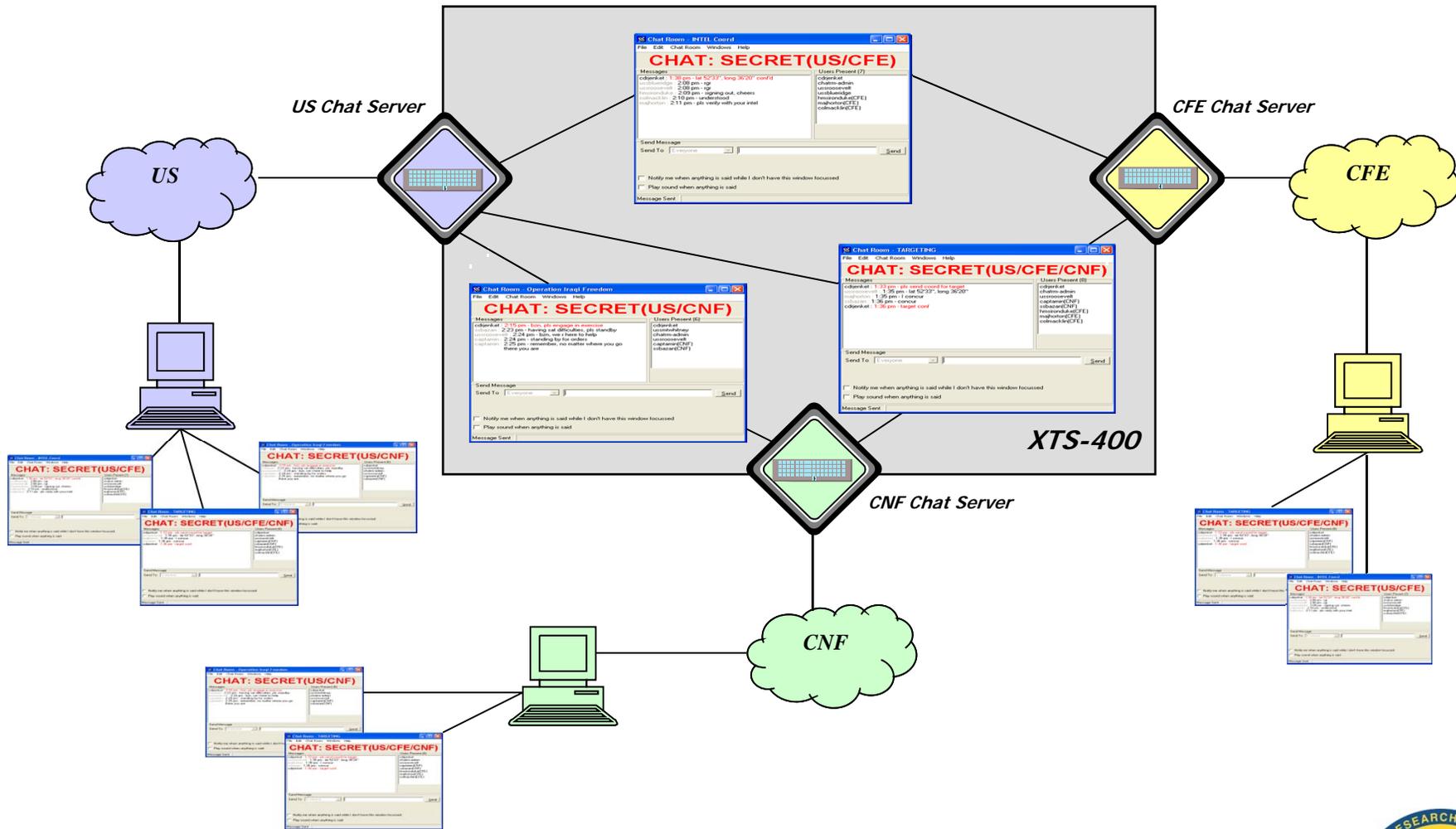
Only the trusted monitor can write to a chat room



- Client interfaces:
 - Native Windows client
 - HTTP-based client/server communications
 - Designed to minimize bandwidth usage
 - Web client
 - True HTTP client/server communications
 - Requires no software installation/upgrades
 - XMPP client
 - Operationally Assessed at C2F in 2006
 - Requires no software installation/upgrades
 - Administrative client
 - Single, multilevel administrative user interface
 - Telnet-based client/server communications protocol



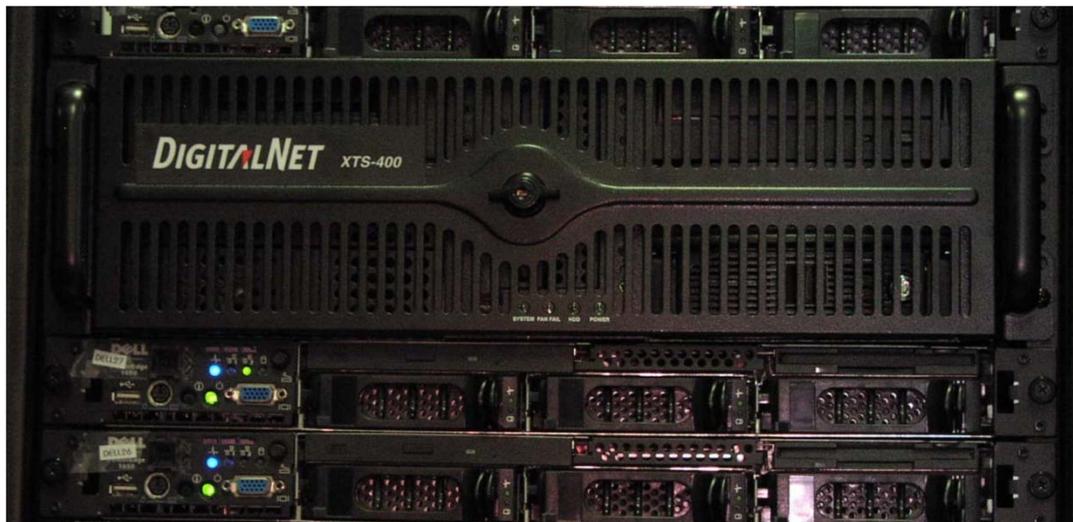
Multilevel Chat: Component Architecture



- **Features:**
 - System runs on a single trusted platform
 - XTS400/410
 - STOP OS Evaluated EAL5+
 - Provides text chat in near real-time
 - Generally within 1 second
 - Scalable
 - Supports up to 15 Network Levels
 - > 500 Users
 - > 50 Chat Rooms
 - Network Interfaces
 - Access:
 - Via existing secure National or Coalition networks
 - Server:
 - Single level chat server instances at each network level



- The Multilevel Chat:
 - The XTS-400 Platform (4U rack mount system)
 - STOP 6.1E Operating System
 - Multilevel Chat Server Software, version 1.0
 - Commercial off the shelf (COTS) Base Collaboration server
 - Government off the shelf (GOTS) MLS/MSL security extensions



XTS-400



- **Certification:**
 - Formal Certification Completed September 2005
 - Included 3 Network Levels
 - Independent Security testing
 - NSA Penetration Testing
 - Security Test and Evaluation Performed at Navy Network Operations Center
 - Listed as MLS Solution on UCDMO Baseline



- Target Environments for Multilevel Chat:
 - Maritime Domain Awareness
 - Ballistic Missile Defense
 - Counter Terrorism
 - Counter Narcotics
 - Humanitarian Assistance
 - Homeland Security
- Need-to-know compartmentalization
 - Intelligence communities
 - Acquisition communities

