Multilevel Web (MLWeb)

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

• Provide the warfighter the ability to share data objects quickly, securely, and cost-effectively across security domains while complying with DoD policies

• Fit into the Service Oriented Architecture (SOA) of the GIG with no changes to existing systems

• Provide an enabling capability for cross-domain, many-to-many communication within a SOA

• Facilitate web-based collaboration between several disparate security enclaves for deployed forces

• Achieve an accreditable system risk rating in both the Genser community and the IC
• Ensure the system will be acceptable to coalition partners; not just to US users
  – Interoperability with coalition systems
  – Sufficient security for coalition accreditation
  – Usability constraints for non-DoD/IC users

• Bridge the Combined, Joint Strategic-Operational-Tactical communications gaps
  – Split staffs, combined Strike groups, etc.
Solution Overview

• System development
  – Based on MLChat’s Hybrid Security Architecture (HSA)
  – Secure, cross-domain *Application* framework
    • Implemented as GOTS
  – Built on/with several proven COTS technologies
• Designed to be a multilevel solution
  – Access, Transfer, and “pure” MLS properties
• STOP 6.4.E is the Trusted Operating System
  – Certain components can be distributed to Linux and/or Windows
• Supports several different data types
  – Based on system policy and site requirements
    • .ppt, .doc, xls, jpg, gif, txt, pdf
    • RFI forms
• Uniquely enables the warfighter to use a COTS client in a single enclave with few or no modifications
• Applies and maintains trusted labels
• Uniquely centralizes enforcement of a security policy
• Enables near-real-time collaboration between large number of separate enclaves
• Can utilize proven products for application services
• No need to maintain separate enclaves for separate coalitions
Trusted vs Untrusted Environment

Trusted Space
- Trusted Monitor
- Web Server
- A-C Container
- ACL
- Writes
- Filter
- Authentication

Untrusted Space
- ACL
- A-B-C Container
- B-C Container
- ACL
- Writes
- Reads

High Integrity Space
- Content Checker
- Policy Decision Engine
- Policy

A User
- Network A
- Reads
- Writes

B User
- Network B
- Reads
- Writes

C User
- Network C
- Reads
- Writes

XTS-400/STOP 6.1
• Connects to existing enclaves and applies a single, unique clearance and label to each network.
• Users set data classifications of content submitted for processing.
  – Access rights based on user’s authentication, network, and privileges.
• Utilizes a guarding mechanism to move labeled data from user’s domain to a multilevel repository.
• Utilizes standards-based and/or COTS applications to extend collaborative web services
  – Posting, replication, retrospective search, etc.
MLWeb: Component Architecture
Hard Problems Solved by MLWeb

• **Data labeling**: Applying a reliable, accurate label to objects that can be processed throughout a system via trusted computing base.

• **Type enforcement**: Reliably ascertaining the data types of objects submitted to a system for processing.

• **Dynamic coalitions**: Allowing for modification of the system policy to reflect real-world relationships between partner nations as their relationships change.

• **Authentication**: Determining the identity of individual users across domains, and associating privileges with those identities.

• **Accreditation**: Provide adequate evidence to obtain necessary connection approvals.

• **Usability**: Users must learn to operate in dynamically changing environments where data labeling and releasability become second nature.
Discretionary Access Controls

- Tied to authentication mechanism
- Implemented on a per-site basis
- Read, Post, Edit privileges configurable
- Integrated site management console
  - Interface served via crossover cable
  - All services are centrally managed
File Posting and Content Checking

- Design uses “plug-in” scheme for content checking modules
- Working with gov’t and industry to balance best-of-breed vs. best practice approaches
- Using CleanContent™ to validate MSOffice files
- GOTS/open source for imagery/compression

Content Checker Architecture
Strong Authentication Example

- Implemented Strong Authentication Web Service
- Based on Arcot WebFort™ technology
- Initially an MSL solution
  - VMs on a Trusted OS
- Target is an enterprise, cross-domain authentication service
- Will be reusable by any interested Cross Domain Solution
Technology Assessment

• Operational Assessment
  – Trident Warrior 09
    • Sponsor COMSECONDFLT
    • Networks: SIPR, JWICS, CMFP
    • Maritime Operational Centers
      – US, Portugal, UK, Canada
  – Received favorable results
    • User survey: MLWeb is useful collaboration tool
  – Certification
    • DIA provided testing and implementation approval
Summary

• A “Multilevel System”
• Provides SOA/coalition portal capability
• Enable secure, distributed collaboration in a network-centric enterprise
• Enable a “fly-away” turn-key coalition collaboration capability
• Designed to support an arbitrarily large number of disparate security enclaves