GENERAL DYNAMICS
C4 Systems

GSAW 2011:
Solving the Cross Domain Command and Control Challenge in Satellite Ground Systems

Anthony Furiga
3/2/2011

Introduction

The goal is to harmonize secure data exchange mechanisms across operational domains to enhance mission execution without hindering flexibility

Cross Domain

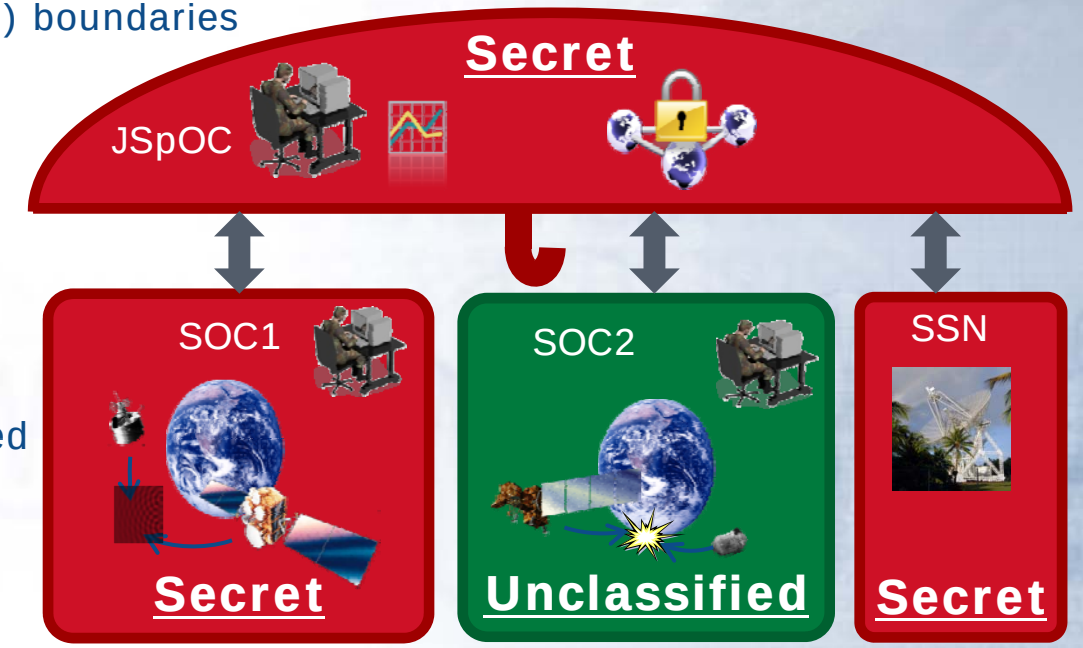
- Data crosses security (and trust) boundaries

Flexible Data Exchange – SOA

- Machine to Machine, highly structured (XML), composable, etc

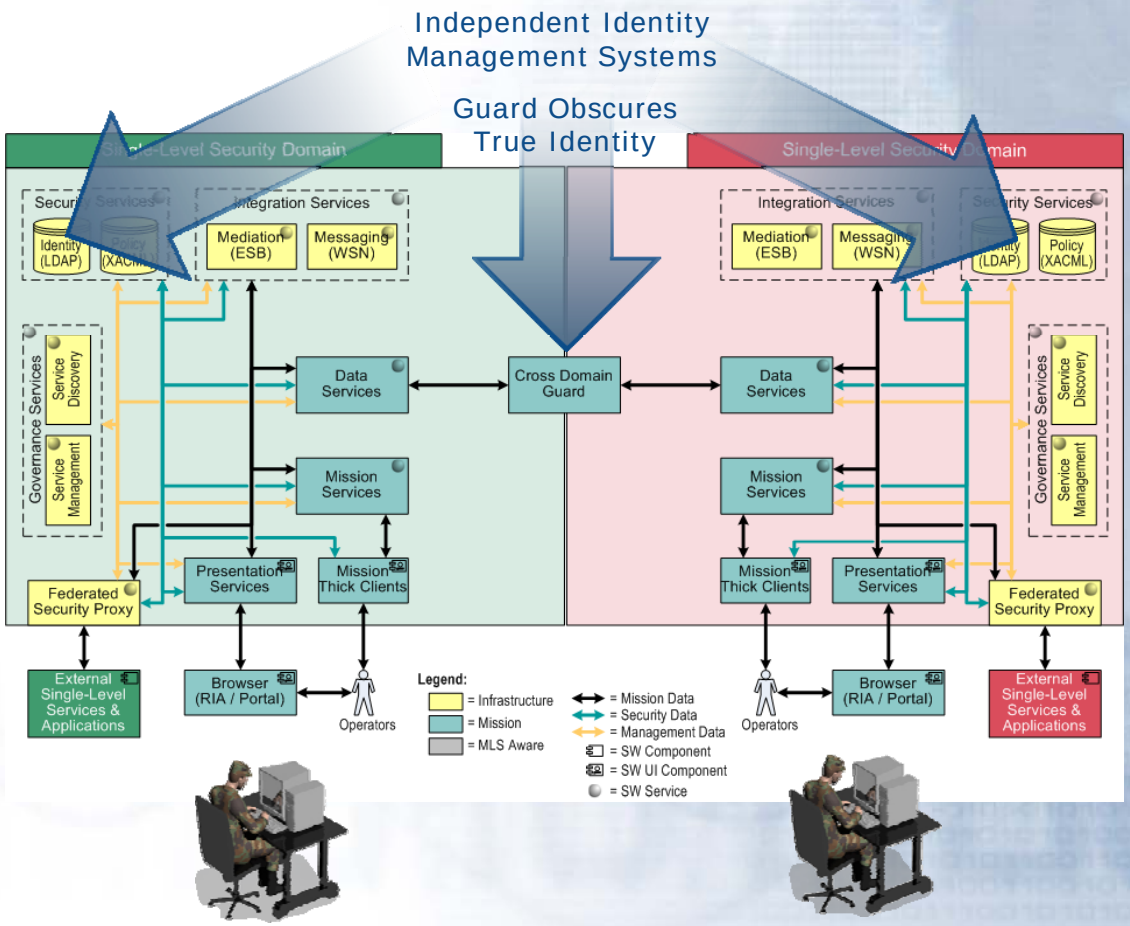
Operational and Secure

- Certifiable–SABI/TSABI approved



Challenge – Single Sign On and Identity Propagation

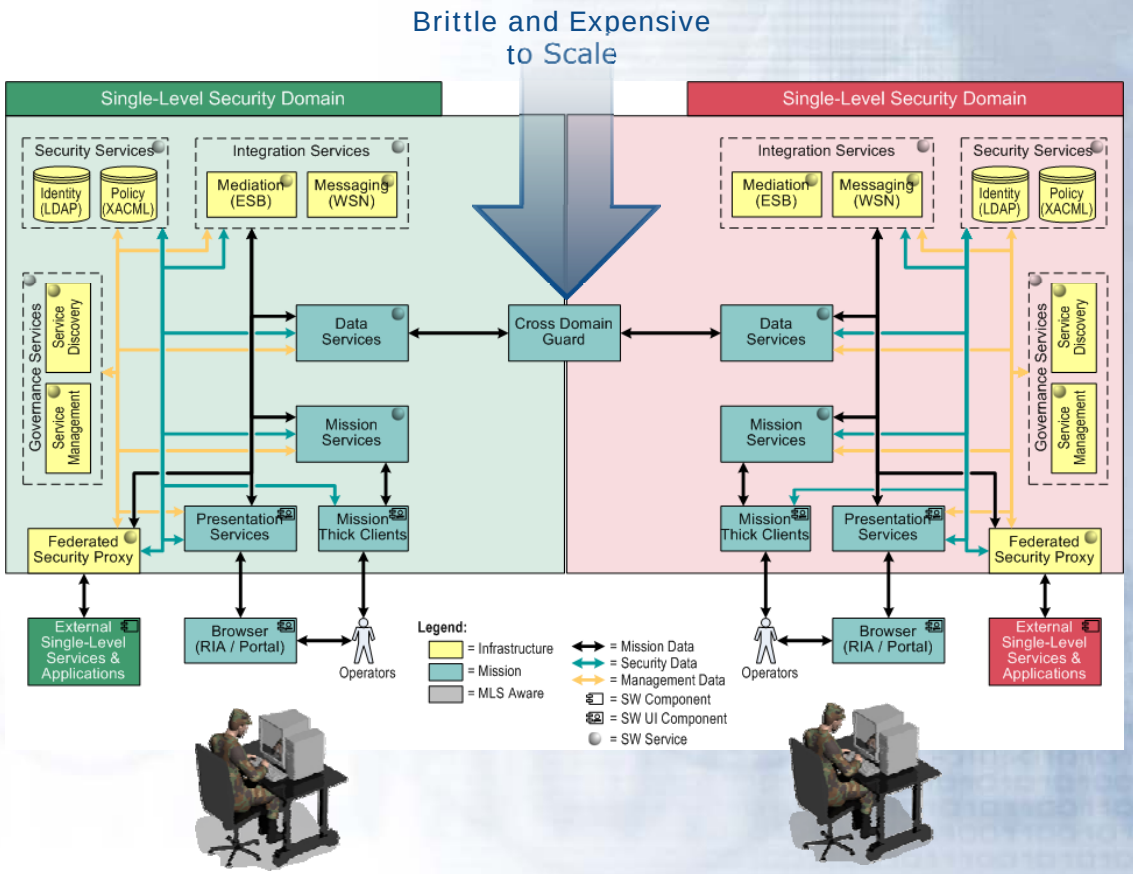
- Case 1: Users must login every time a layered service crosses a security boundary.
- Case 2: Configure system accounts to avoid multiple boundary logins BUT:
  - Identity of the original user is lost and auditing is more difficult
  - Authorization becomes “coarse” because everyone gets treated the same with a common account



GENERAL DYNAMICS
C4 Systems

Challenge - The current approaches don't support evolving mission requirements

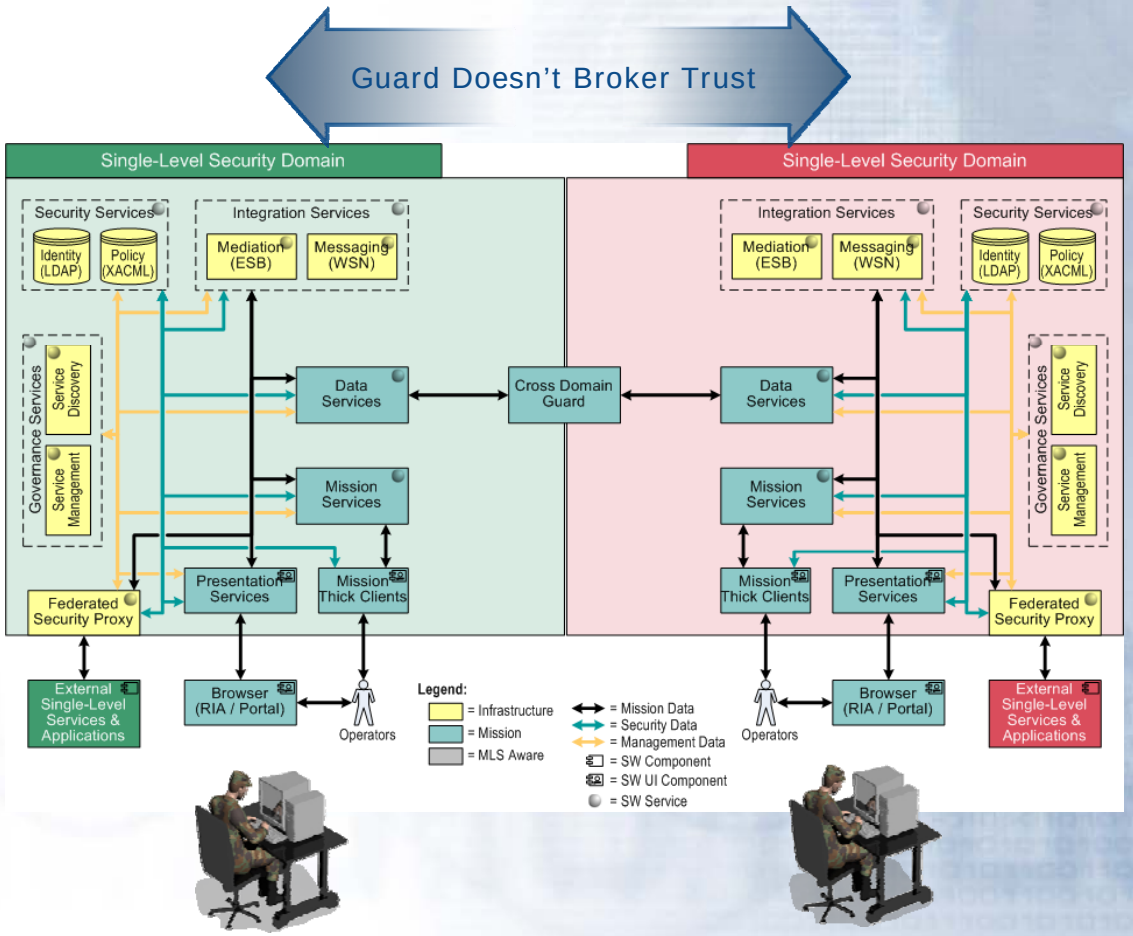
- Cross Domain guards on their own are brittle and don't support even the smallest of changes:
  - Data flows must be known prior to runtime
  - Changes take months, new SABI/TSABI approval cycles
- Cross Domain guards are point-to-point – don't scale well!
  - New Cross Domain guard is required per interface/domain



GENERAL DYNAMICS
C4 Systems

Challenge – Cross Domain Trust

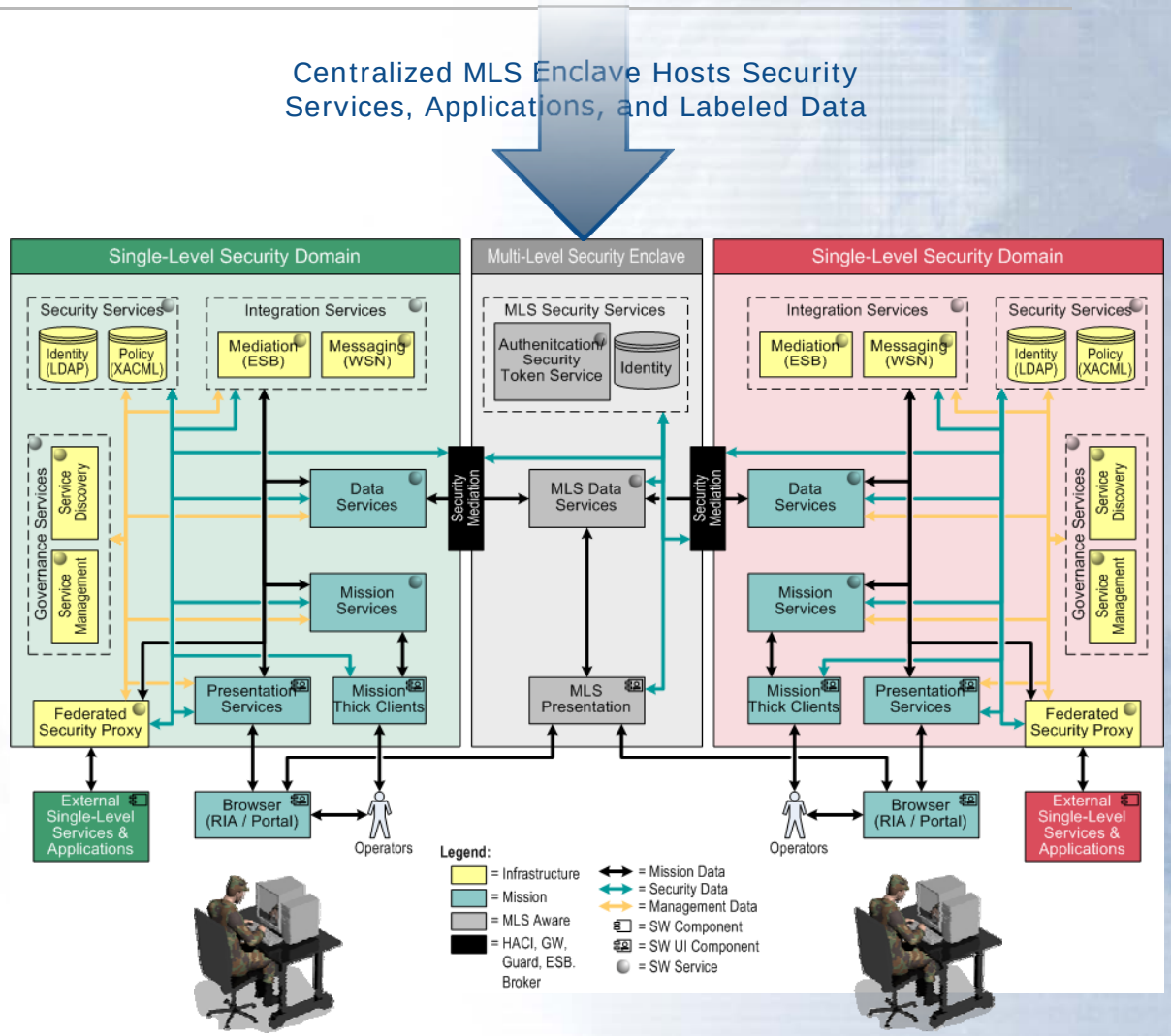
- Guard doesn't "broker trust" between domains, the domains are delegating authority to the guard:
  - PKI domains terminate
  - Authentication assertions from one domain are not useful in other domains



GENERAL DYNAMICS
C4 Systems

Trusted MLS Enclave Approach – Challenges Addressed

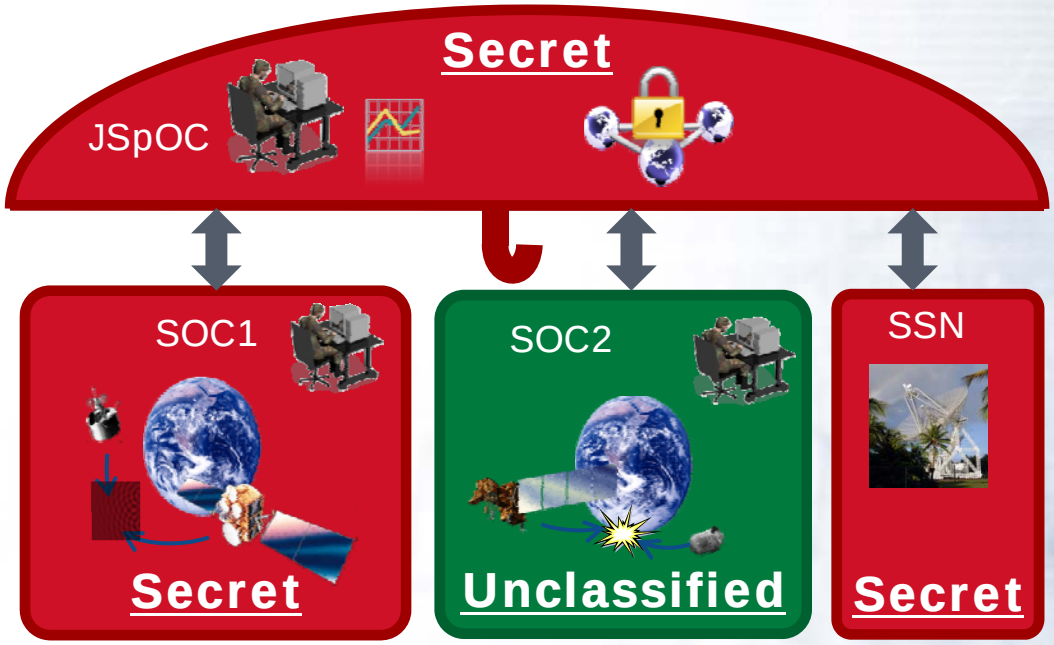
- Trusted MLS Secure Enclave provides:
  - Controlled access to MLS aware applications and data
  - Authentication and Federated Identity services
- Single Sign-On and Identity Propagation are handled via Security Token Service (SAML assertions signed by the trusted source) which gets attached to the composite mission service invocations
- Changes to services can be accommodated without changes to MLS interfaces
- Scales well as new domains and users increase over time



GENERAL DYNAMICS
C4 Systems

Video Demonstration

- Cross Domain Transfer



Key Technologies and Products

- PKI
  - Identity and Trust (CA)
- XML Schema, XML Signature, IC-ISM XML Schema
  - Data format and content labeling
- SAML
  - Single Sign-On, Identity Propagation
- WS-* Standards
  - Secure/Standards based interfaces
- Layer7 Secure Span Gateway
  - Security Proxy
- Oracle 11g
  - Application Servers, ESB
- General Dynamics Trusted Network Environment
  - Trusted MLS Secure Enclave (data broker)
- General Dynamics TacGuard XD
  - Cross Domain Guard

Summary

- The cross domain transfer (i.e. guards) approach to sharing data “across domains” has significant limitations
- By integrating a centralized, trusted MLS secure enclave data broker (COTS product) with existing technologies, these problems can be solved
- When architected correctly, MLS cross-domain transfer can appear to be like any other SOA service and therefore take advantage of a service architecture to provided enhanced mission execution – allows sharing without a priori knowledge