ALION
SCIENCE AND TECHNOLOGY
Aligned with your needs.

Towards a Reference Architecture for Service-Oriented Cross Domain Security Infrastructures

Wen Zhu
Dr. Lowell Vizenor
Dr. Avinash Srinivasan

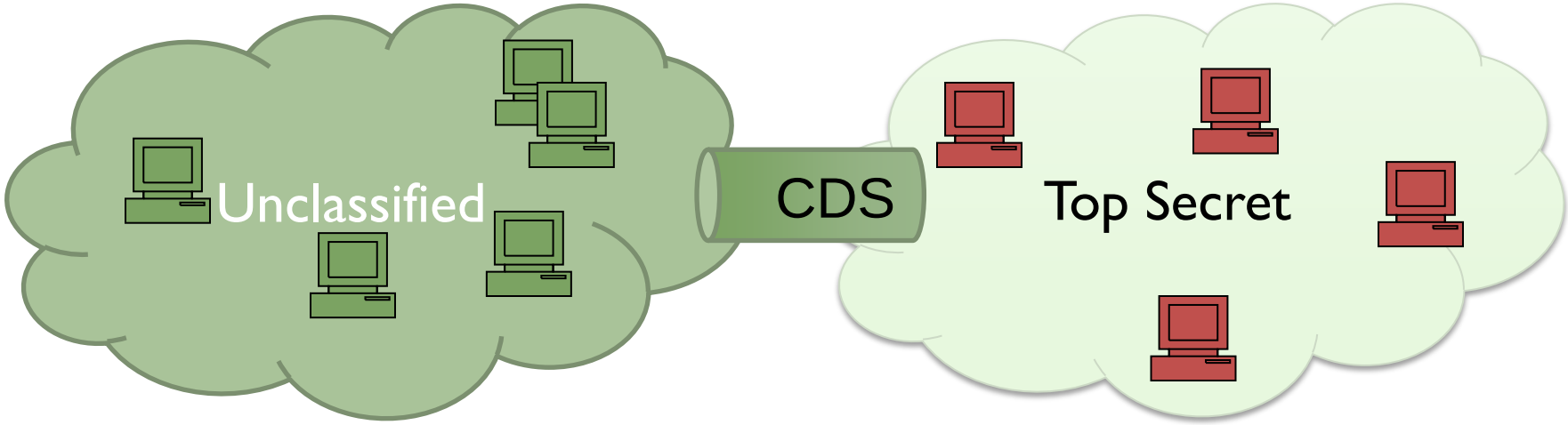
7th International Conference on Internet and Distributed Computing Systems

Agenda

- Background
  - Issues with Current Solutions
  - Example Use Case
- CDS Reference Architecture
  - Reference Architecture concerns
  - CDC Participants
  - CDS Protocol Candidates
- Putting It Together

Background

- Security Domain:
  - Protection based on the classification and sensitivity of data
  - Within each domain, a certain level of trust is assumed
- Cross Domain Solutions
  - Filter and inspect traffic cross domain boundaries
  - Primary consist of Guards that monitors communication channels



Issues with Guard Implementations Today

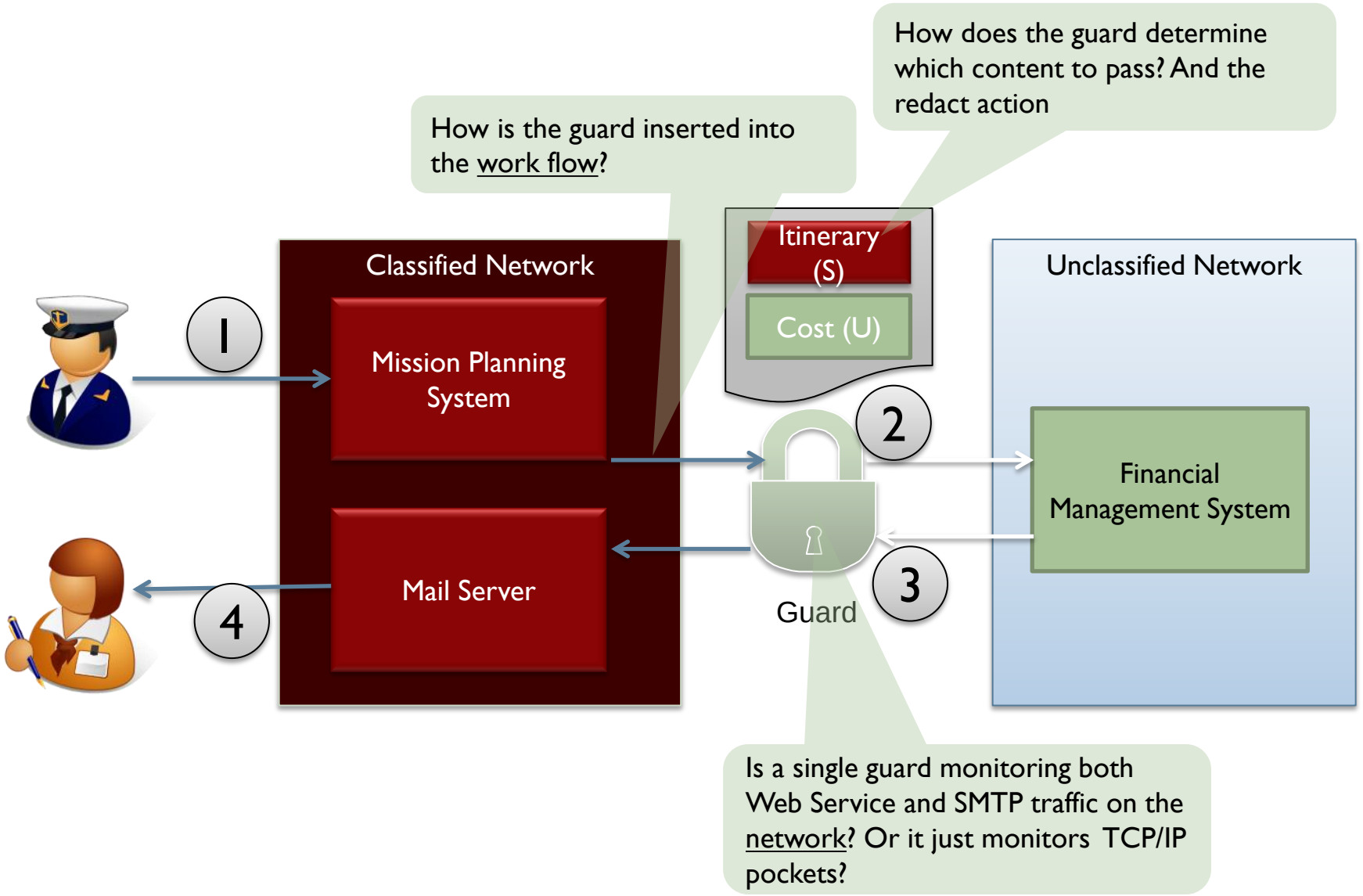
- Mission applications design perspective
  - Programs to design and implement their own individual solutions
  - No support workflows or full-duplex architectures
- Enterprise security infrastructure perspective
  - Commonly associated with the links between domains
  - CDS vendors define the mission application interfaces
  - Limited configurability and API
  - Lack of protocol for coordination among guards
- Effectiveness and performance perspective
  - Lack of a standard and flexible framework for describing information

CDC in the Context of Service Oriented Architecture (SOA)

- SOA Practices
  - Communication at the application layer
  - Complex workflow
  - Rich metadata (service description and policy)
  - End-to-end security
  - Standard-based interoperability

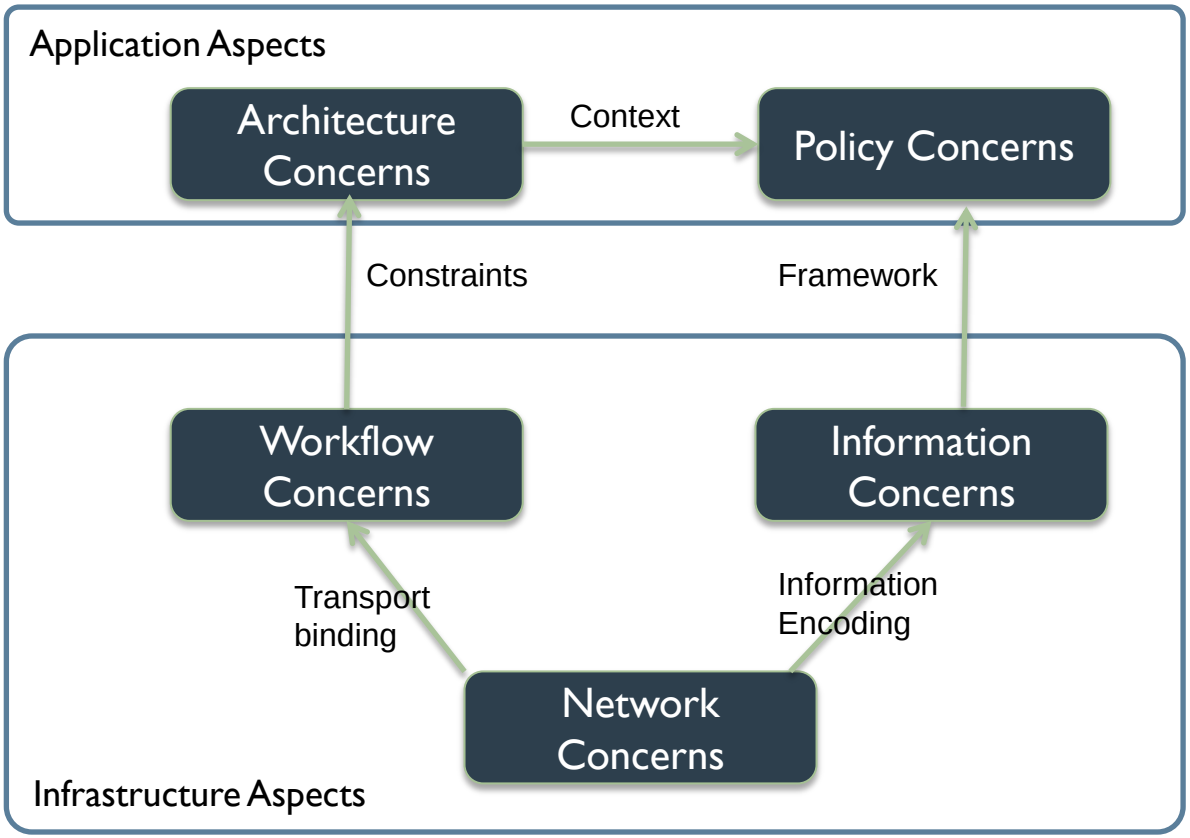
- Current Guards Capabilities
  - Inspection at the transport layer
  - Not participate in workflow
  - Based on message context
  - Communication link
  - Lack of common standards

Example Use Case: Approval of Classified Travel



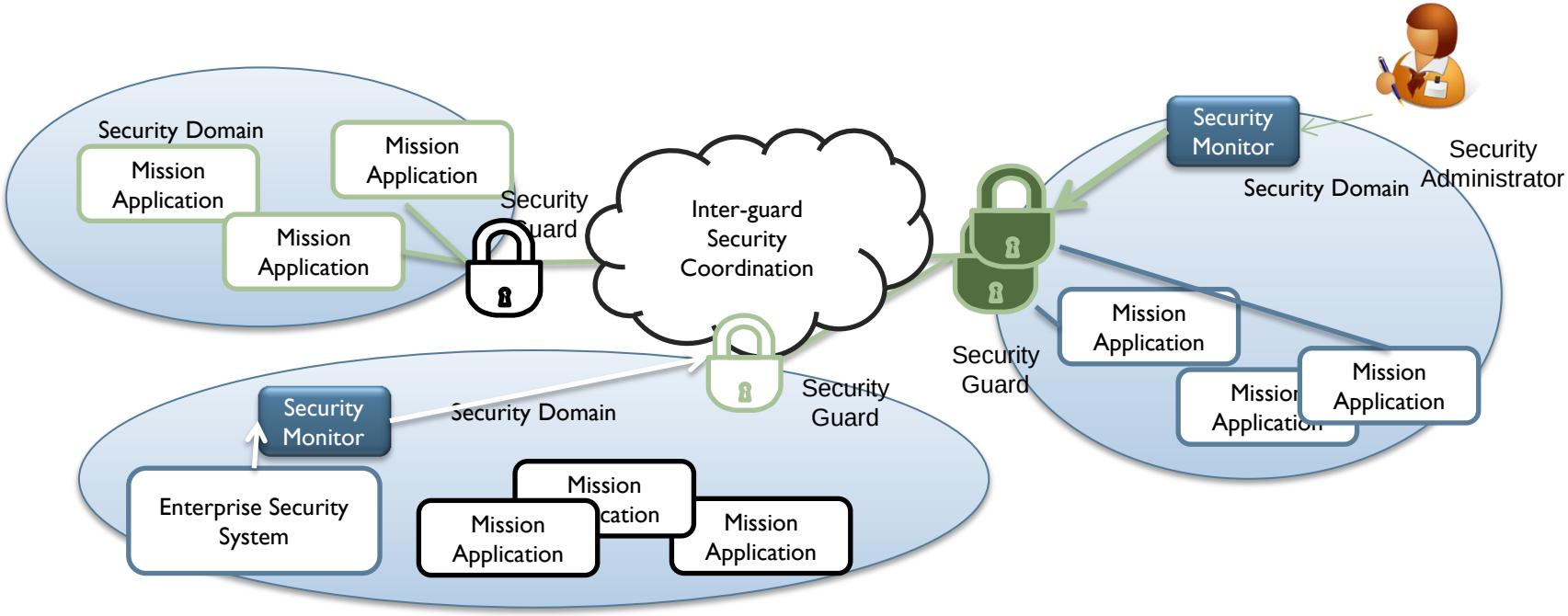
CDS Reference Architecture

- The reference architect will provide
  - A framework for discussing multi-faceted concerns of CDS
  - A context in which interactions among CDS participants can be abstracted out, forming the basis for protocols



CDS Participants

- Security Domain
  - Implies a consistent a security vocabulary for users (human and systems), activities and information
- Security Monitor (Optional)
  - Defines consistent security policies for communication with other domains using the security vocabulary.
- Mission Application
  - Associate mission-specific concepts with the security vocabulary.
- Security Guard
  - Enforces security policy defined by the mission application. MAY act a Policy Enforcement Point for the domain.

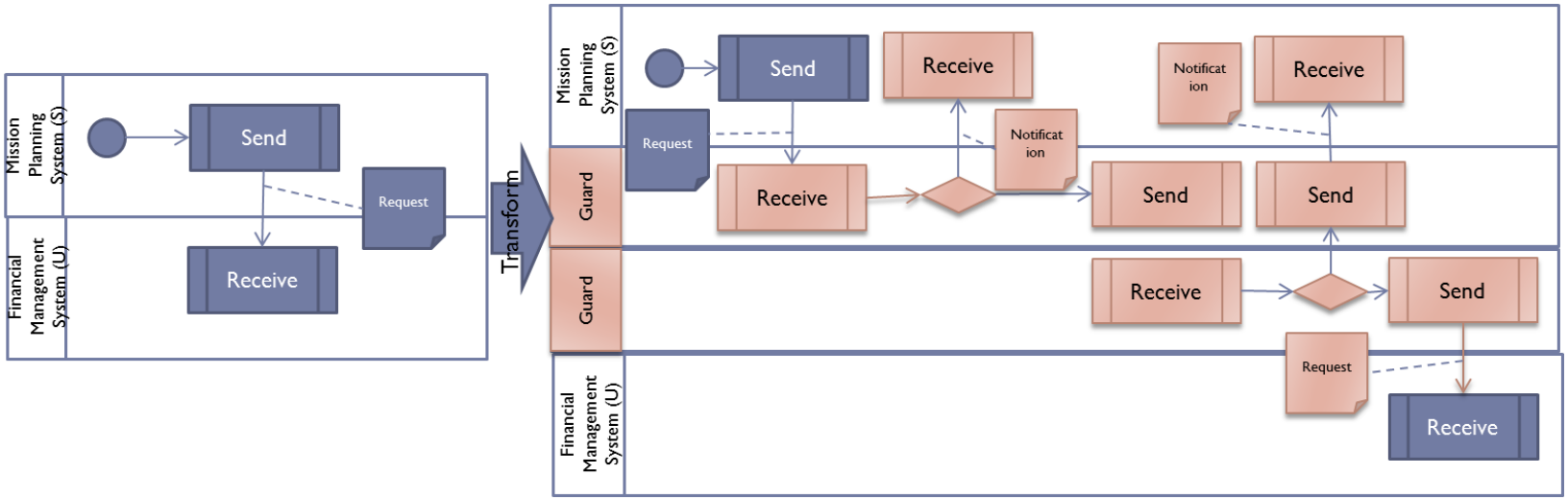


Associating Guards with Security Domains

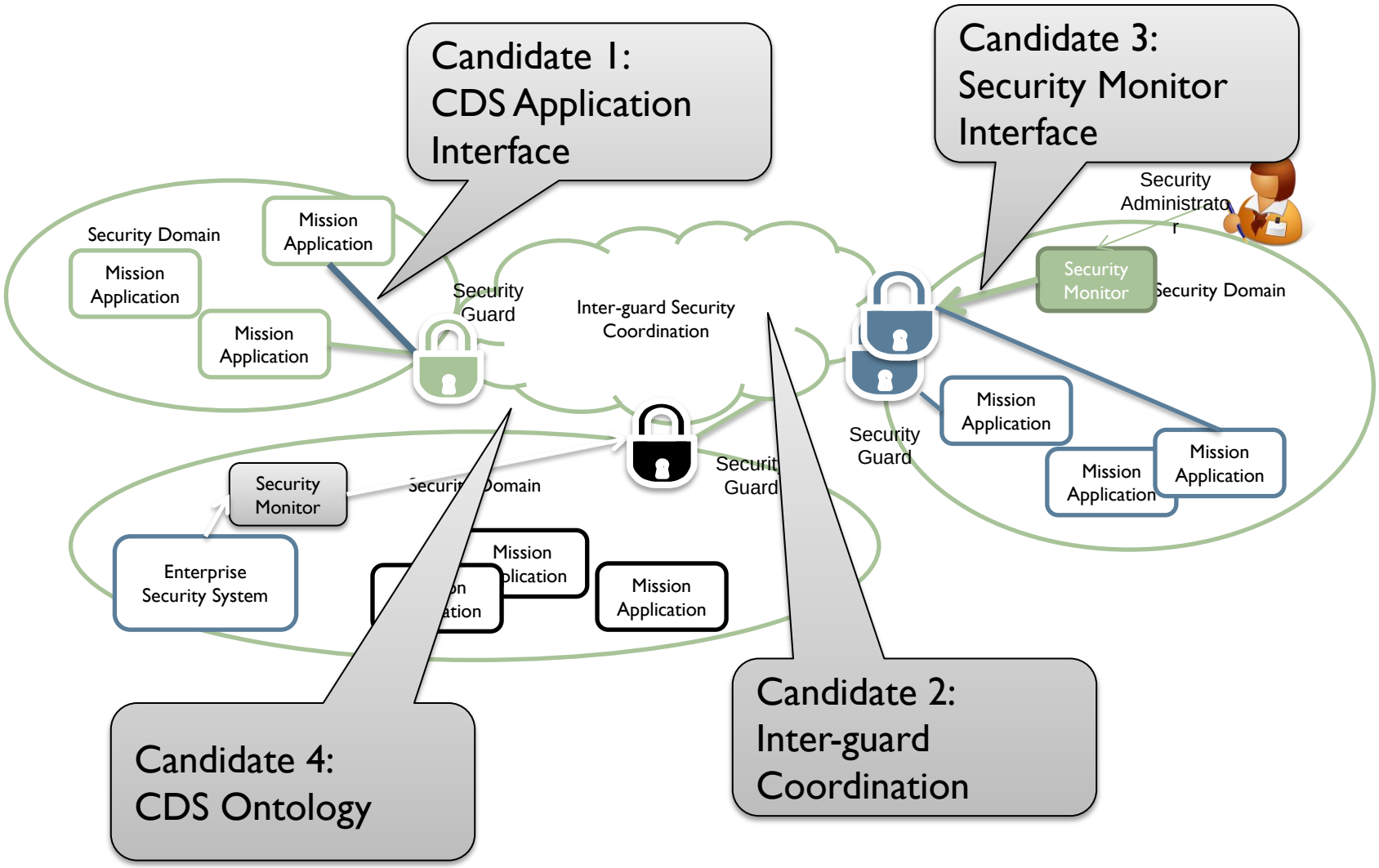
- A Guard SHOULD be associated with a single Domain.
  - Security:
    - Guard operates at the same security level as the associated Domain without unnecessary privilege
    - The same security monitor (system and human operator) manages both the domain and the guard, avoiding policy conflicts and duplication
  - Scalability:
    - Avoid n square problem in a multi domain environment
  - Implication:
    - Guards needs to trust each other without revealing mission information each other

Guards as Active Participants in Workflow

- Mission applications MUST be aware of the guards and communicate explicitly with the guard
  - Need a notification mechanism in case a message is blocked by the guard for the security reasons.
  - End-to-end encryption may prevent the guard from inspecting the
  - Covert Channels will be impossible if the guard actively intercept and forward the message.
- A Guard MAY provide additional information management services to mission applications
- BPMN/BPEL could be extended to model the guards as part of the work flow



Opportunity for Standardizing Interactions – CDS Protocol Candidates



Putting It Together