Policy Overlay Networks

Christopher C. Lamb

Department of Electrical and Computer Engineering
University of New Mexico

June 10, 2011

THE UNIVERSITY of NEW MEXICO

Outline

Introduction

Distributed enterprise computing systems are facing a troubling future. They are:

- *Expensive* — They do not use current commercial resources and use costly partitioning schemes
- *Unreliable* — Too reliant on outmoded security approaches
- *Slow* — Sensitive information is manually reviewed too often leading to the right people being unable to get the right information in time

They need to be re-imagined to take advantage of radical shifts in computational provisioning.

Federal computer systems are a prime example of these kind of problematic distributed systems, and demonstrate the difficulty in implementing new technical solutions.

The Problems — Customer Perspectives

Current policy-centric systems are being forced to move to cloud environments and build much more open systems. Usage management is a key problem in this domain — information needs to be delivered to those who need it as soon as possible:

"...It is imperative to effectively exchange information among components, Federal agencies, coalition partners, foreign governments and international organizations as a critical element of our efforts to defend the nation and execute national strategy..." [**?**]

— *DoD Information Sharing Strategy*

"...The CIO of the National Security Agency is focusing on IT architecture and a cloud-centric approach to sharing information..." [**?**]

— *Informationweek*

The Problem — Characteristics

Cloud systems may save money, provide more flexibility, but they also [**?**]:

- *Are Not Private* — User data control in SaaS is lacking, causing policy concerns for agencies; Data owners have no technical control over secondary use; providers may use offshore development; data can be routed across sensitive countries or secondarily stored on CDNs; data privacy on bankruptcy is ill-defined
- *Are Less Secure* — Controlling data access, data may not be wiped in all XaaS scenarios, availability/backup leads to possible data proliferation, lack of standardization in intercloud communication and data transfer, multi-tenancy and side-channel attacks, difficult logging/auditing
- *Cannot Be Trusted* — Trust relationships, consumer trust

Current Solutions

How are these problems being addressed by impacted organizations?

They're just starting to be actively addressed and are an open research question [**?**].

Cross-domain architectures are currently the standard for monitoring and information dissemination in an effort lead by the *Unified Cross Domain Management Office*, associated with the Department of Defense (DoD) and the National Security Agency (NSA).

Current Solutions — NSA

Legacy cross-domain notional architecture [**?**]

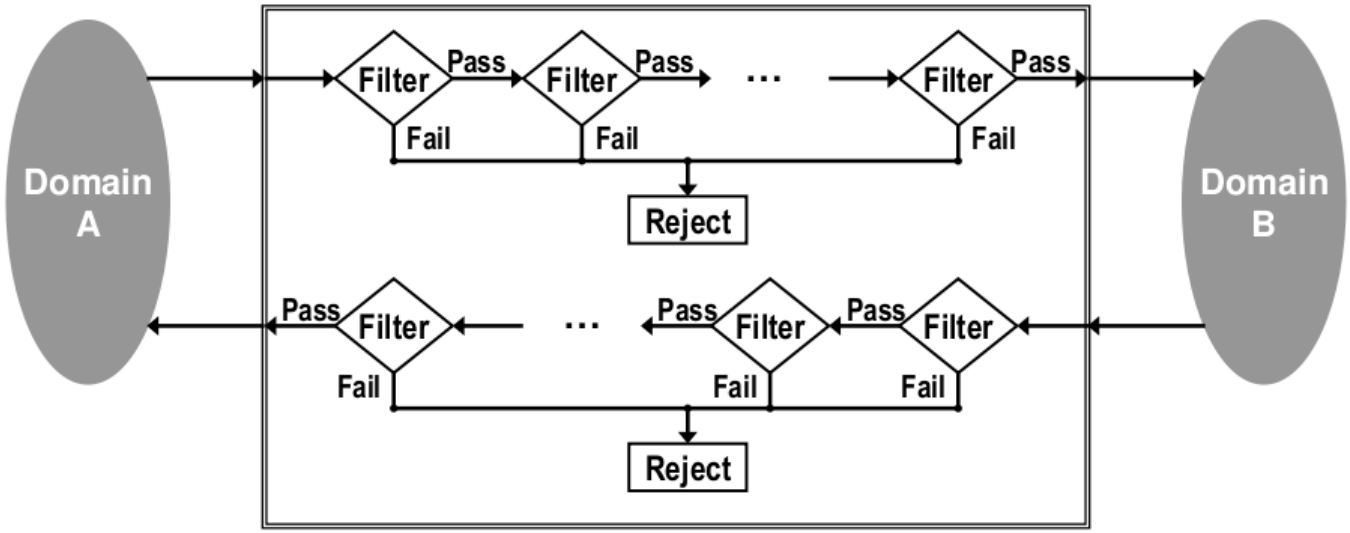

Figure: NSA Legacy Model

Domain A — Private cloud managed by the Air Force
Domain B — A public operational network

Current Solutions — NSA (SoA)

Future cross-domain notional architecture [**?**]

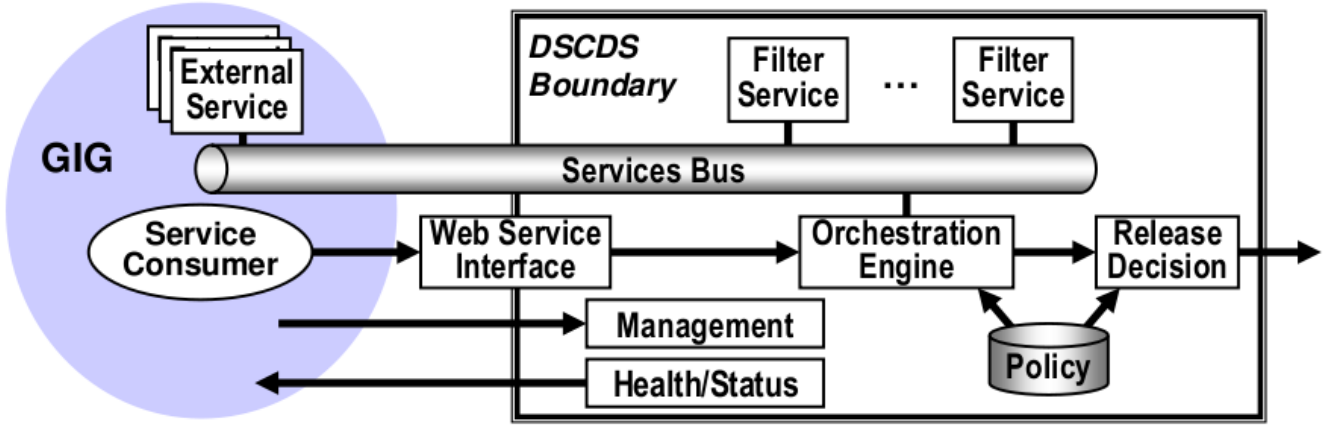

Figure: NSA Service-Oriented Model

GiG — Global Information Grid; a large public cloud operated by the DoD
DSCDS — Distributed Service-oriented Cross Domain Solution

Current Solutions — Raytheon

Raytheon's notional architecture supporting cross-domain information flow [**?**]:

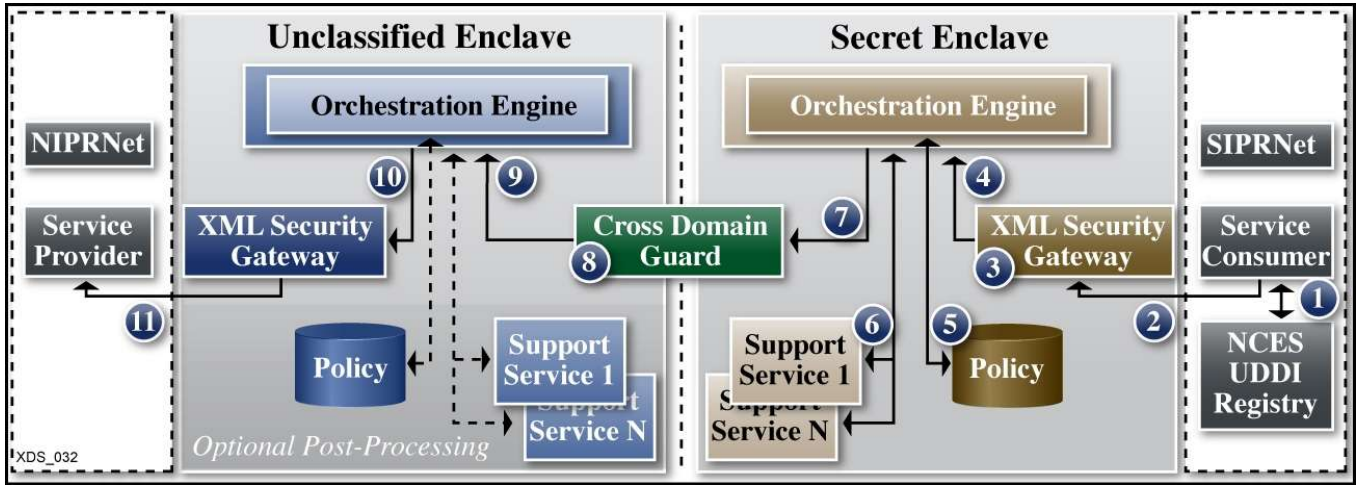

Figure: Raytheon Model

...still uses a single perimeter guard...

Current Solutions — BAH

Booz—Allen—Hamilton presented a service-centric cross domain solution in 2009 [**?**]:

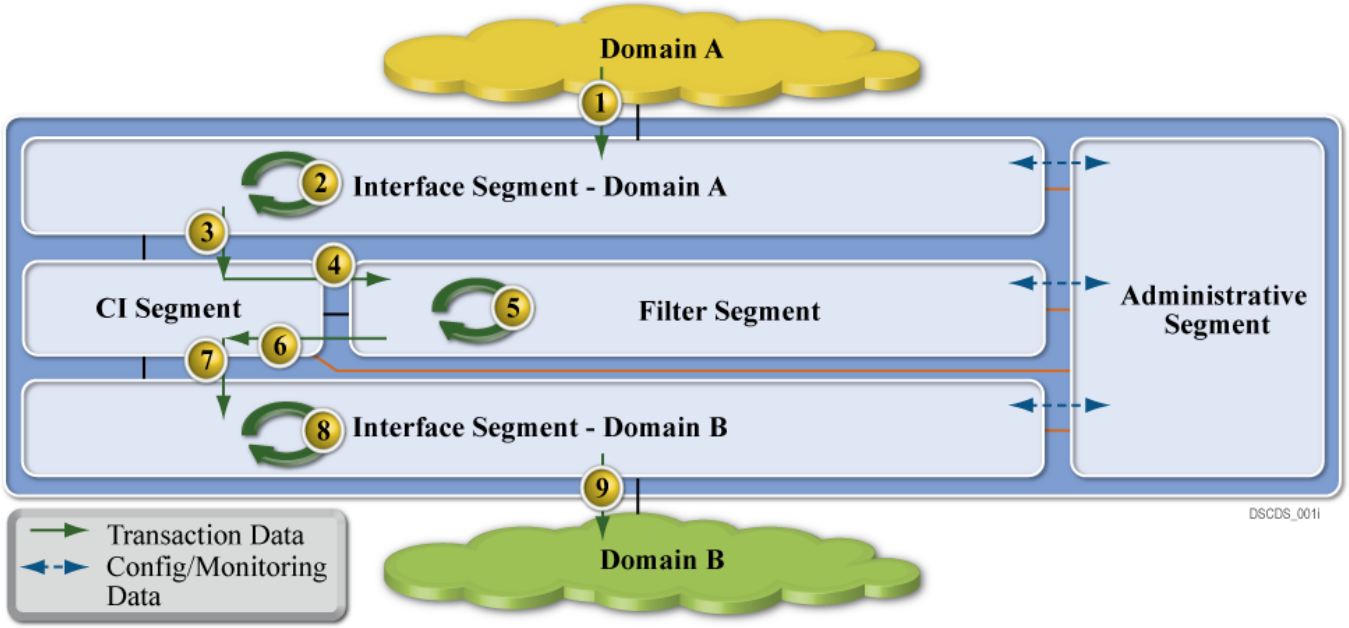

Figure: Booz—Allen—Hamilton Model

...still uses a single perimeter guard (called a filter segment)...

Future Solution

Organizations are falling back on what they know in the scope of new problems.

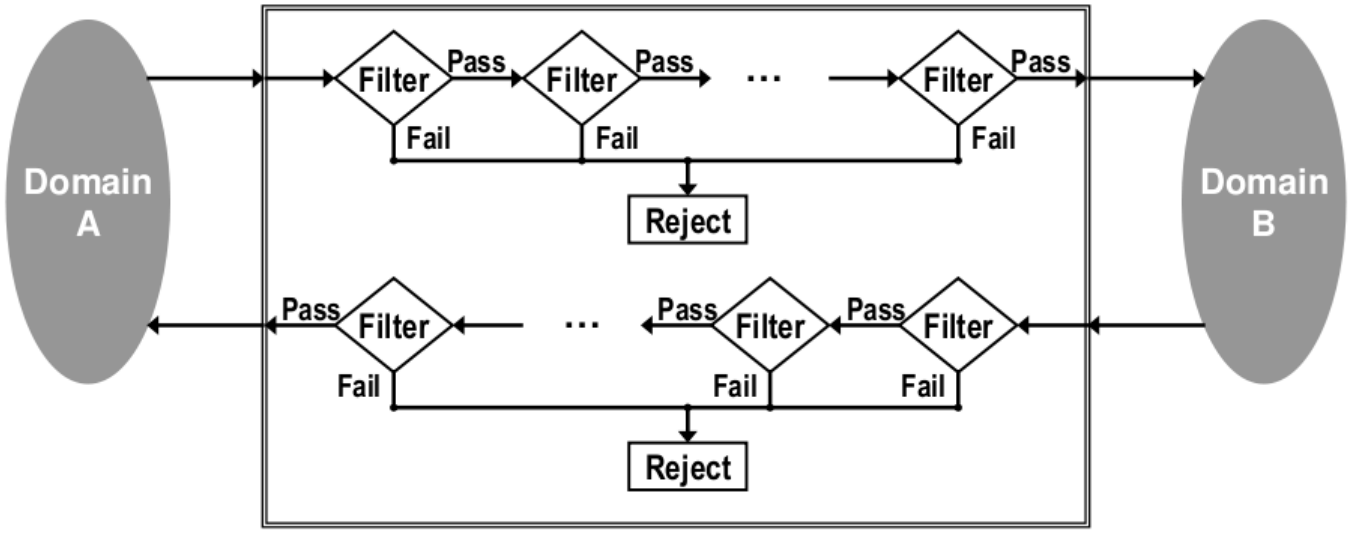

Figure: NSA Legacy Model

Even though we know they don't work [**?**].

Characteristics of Current Solutions

- *Centralized Policy* — They use centralized policy injection into communication flow. Note that in each sample model, policy is *only* evaluated at guard points.
- *Physical to Compartment Mapping* — In each of these cases, users are only allowed to exchange one type of information per domain. The physical domain systems are locked (by operational policy) to a single classification level limit. Users cannot, for example, have *Top Secret* material on a network accredited for *Secret* material.
- *Perimeter Protection* — The use of a single policy enforcement point at domain interconnects supplies a crunchy exterior to the creamy interior data filling.

What's Wrong with Current Solutions?

- *Centralized Policy* — A centralized policy enforcement system simplifies infrastructural attacks. Adversaries know exactly where to focus efforts to compromise policy enforcement, lowering overall system trustworthiness and reliability.
- *Physical to Compartment Mapping* — The traditional model for multi-level security, enforced in this scheme, is that the network is classified at the level of the most sensitive data that transits it. Ergo, those that have clearances at a level to view sensitive data are unable to view that data generally without extensive swivel-chair integration.
- *Perimeter Protection* — Perimeter protection is a necessary but not sufficient security approach. By itself, it doesn't work [**?**].

Characteristics of Future Solutions

- *Decentralized Policy* — Policy management is decentralized and integrated within the fabric of the system. The system is both more secure and resilient as a result, better able to control information and operate under stressful conditions.
- *Infrastructure Reuse* — Multi-tenancy can lower costs and increase reliability and is furthermore a common attribute of cloud systems. An appropriately secured system facilitates integration of computing resources into multi-tenant environments.

Characteristics of Future Solutions

- *Cloud Integration* — The ability to handle multi-tenant environments and to reliably secure both data at rest and data in motion leads to computational environments deployable in cloud systems.
- *Security in Depth* — Systems must operate under *all* conditions, including when they are under attack or compromise [**?**]. Ergo, they must provide protection to sensitive data in depth.

Related Work

TBD

System Architecture

What would this kind of overlay system look like?

- *Meta-Model*
- *Non-Hierarchical Overlays*
- *Hierarchical Overlays*
- *Ontologies and Taxonomies*

...and what would the migration path to these systems look like?

System Architecture - Level 0

Level 0 system

Current generation solutions
Perimeter Security
Physical Networks Only
Centralized Policies

System Architecture - Level 1

Level 1 system

Decentralized Policy Management

System Architecture - Level 2

Level 2 system

Integrated Policy Awareness

System Architecture - Level 3

Level 3 system

Fully Integrated Policy Aware Decentralized System

Conclusions

Contribution of Work

The unique contribution of this work is a quantitative analysis of policy-centric overlay network options, associated taxonomies of use, and prototypical technology prototypes.

- *Overlay Options* — This includes various types of overlay networks and associated strengths and weaknesses addressing centralized and decentralized models
- *Taxonomies of Use* — Depending on the specific usage management requirements and context, different overlays have different applicability; this work will provide guidance on suitability
- *Prototypical Technologies* — Examples and proofs-of-concept will be required to appropriately analyze various architectural alternatives

Questions?

THE UNIVERSITY of
NEW MEXICO