# 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

THE UNIVERSITY of
NEW MEXICO

# Introduction

# The Problem — Customer Perspectives

Current policy-centric systems are being forced to move to cloud environments and build much more open systems:

"...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..."[1]
— *DoD Information Sharing Strategy*

"...The CIO of the National Security Agency is focusing on IT architecture and a cloud-centric approach to sharing information..."[2]
— *Informationweek*

# The Problem — Characteristics

Cloud systems may save money, provide more flexibility, but they also [6]:

- *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* — Data owners no longer completely control data access, data may not be wiped in all XaaS scenarios, availability and backup leads to possible data proliferation, lack of standardization in intercloud communication and data transfer, multi-tenancy exposure to side-channel attacks, difficulty with reliable logging and auditing

- *Cannot Be Trusted* — Trust relationships, consumer trust

# The Problem — Characteristics

Cloud systems may save money, provide more flexibility, but they also [6]:

- *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* — Data owners no longer completely control data access, data may not be wiped in all XaaS scenarios, availability and backup leads to possible data proliferation, lack of standardization in intercloud communication and data transfer, multi-tenancy exposure to side-channel attacks, difficulty with reliable logging and auditing

- *Cannot Be Trusted* — Trust relationships, consumer trust

THE UNIVERSITY of
NEW MEXICO

# The Problem — Characteristics

Cloud systems may save money, provide more flexibility, but they also [6]:

- *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* — Data owners no longer completely control data access, data may not be wiped in all XaaS scenarios, availability and backup leads to possible data proliferation, lack of standardization in intercloud communication and data transfer, multi-tenancy exposure to side-channel attacks, difficulty with reliable logging and auditing

- *Cannot Be Trusted* — Trust relationships, consumer trust

# The Problem — Characteristics

Cloud systems may save money, provide more flexibility, but they also [6]:

- *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* — Data owners no longer completely control data access, data may not be wiped in all XaaS scenarios, availability and backup leads to possible data proliferation, lack of standardization in intercloud communication and data transfer, multi-tenancy exposure to side-channel attacks, difficulty with reliable logging and auditing

- *Cannot Be Trusted* — Trust relationships, consumer trust

# Current Solutions — NSA
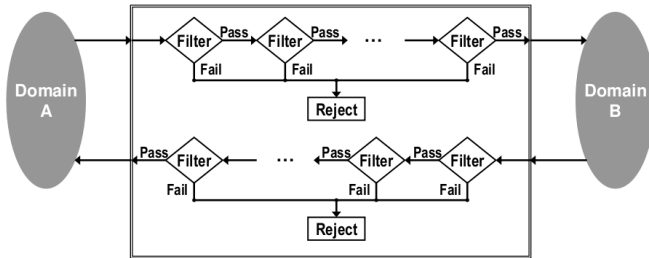
Legacy cross-domain notional architecture [4]



Figure: NSA Legacy Model

# Current Solutions — NSA (SoA)

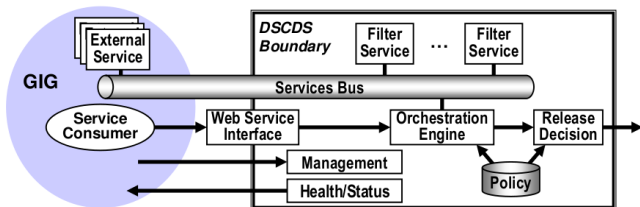Future cross-domain notional architecture [4]



Figure: NSA Service-Oriented Model

# Current Solutions — Raytheon

Raytheon's notional architecture supporting cross-domain information flow [5]:
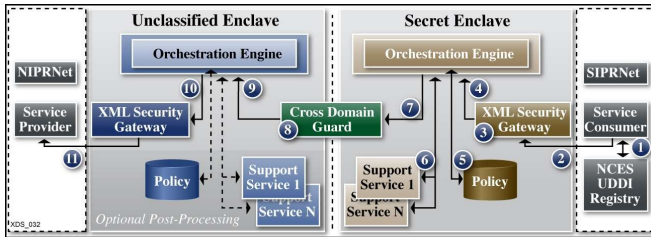


Figure: Raytheon Model

# Current Solutions — BAH

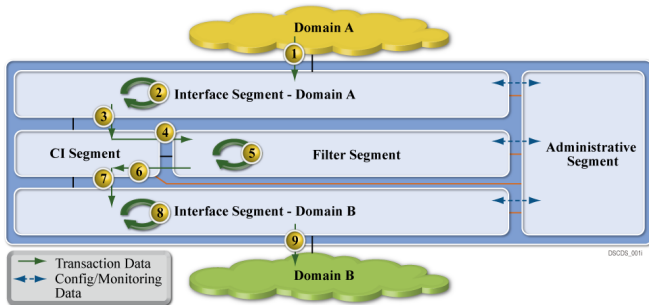Booz—Allen—Hamilton presented a service-centric cross domain solution in 2009 [3]:



Figure: Booz—Allen—Hamilton Model

[1] DoD Information Sharing Strategy.
http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf, May 2007.

[2] NSA Pursues Intelligence-Sharing Architecture.
http://www.informationweek.com/news/government/cloud-saas/229401646, April
2011.

[3] Booz, Allen, and Hamilton. Distributed service oriented architecture
(soa) compatible cross domain service (dscds). Presented at the
Unified Cross Domain Management Office Conference, 2009.

[4] NSA. Distributed service oriented architecture (soa)- compatible
cross domain service (dscds) dscds overview. Presented at the Unified
Cross Domain Management Office Conference, 2009.

[5] J. Ostermann. Raytheon dscds intro. Presented at the Unified Cross
Domain Management Office Conference, 2009.

[6] S. Pearson and A. Benameur. Privacy, security and trust issues
arising from cloud computing. In *Cloud Computing Technology and
Science (CloudCom), 2010 IEEE Second International Conference on*,
pages 693 –702, 30 2010-dec. 3 2010.

THE UNIVERSITY of
NEW MEXICO