Ten years of Layered Assurance at Galois, lessons learned, and looking forward

Dylan McNamee
Galois, Inc.
dylan@galois.com

Layered Assurance Workshop

December 7, 2015

galois

Overview

- How Galois got here
- Some lessons we learned
  - implementation language factors
  - decomposition surprises
  - managing theorem proving
  - complex path to market
- Some challenges we see

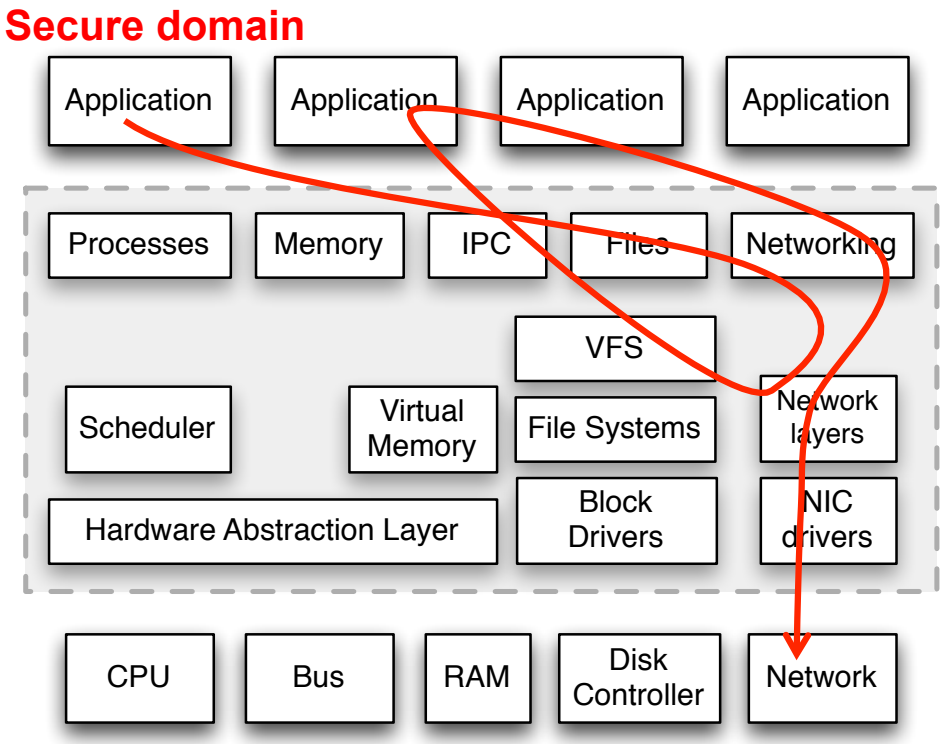
| galois |

Market opportunity: bad reference monitors

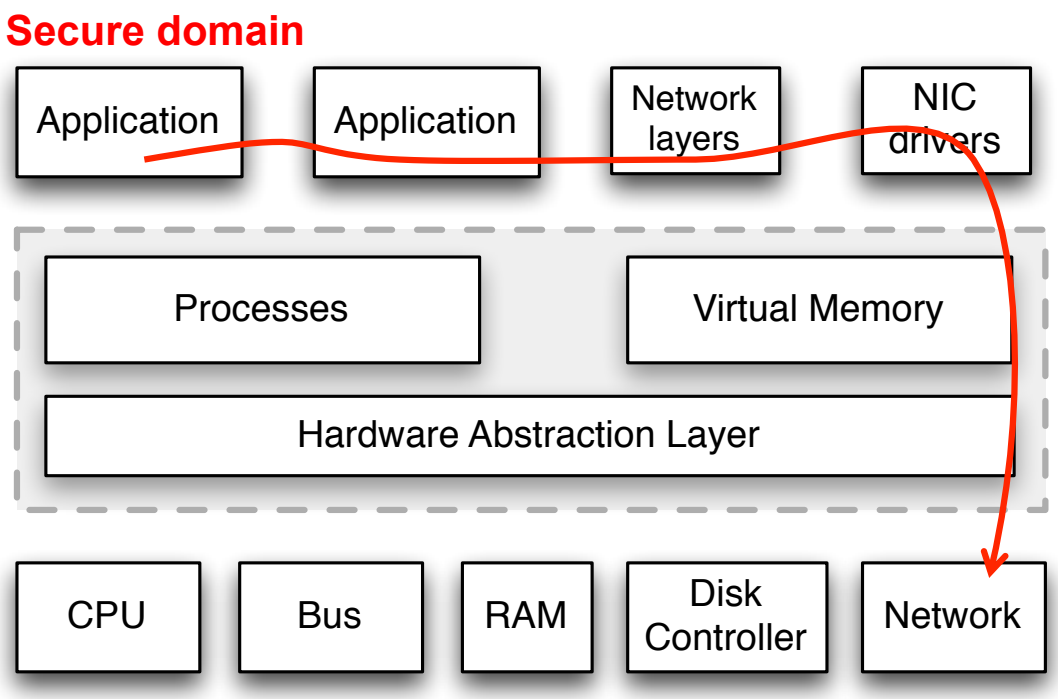
Another bad reference monitor

Motivation for MILS' approach to reference monitors

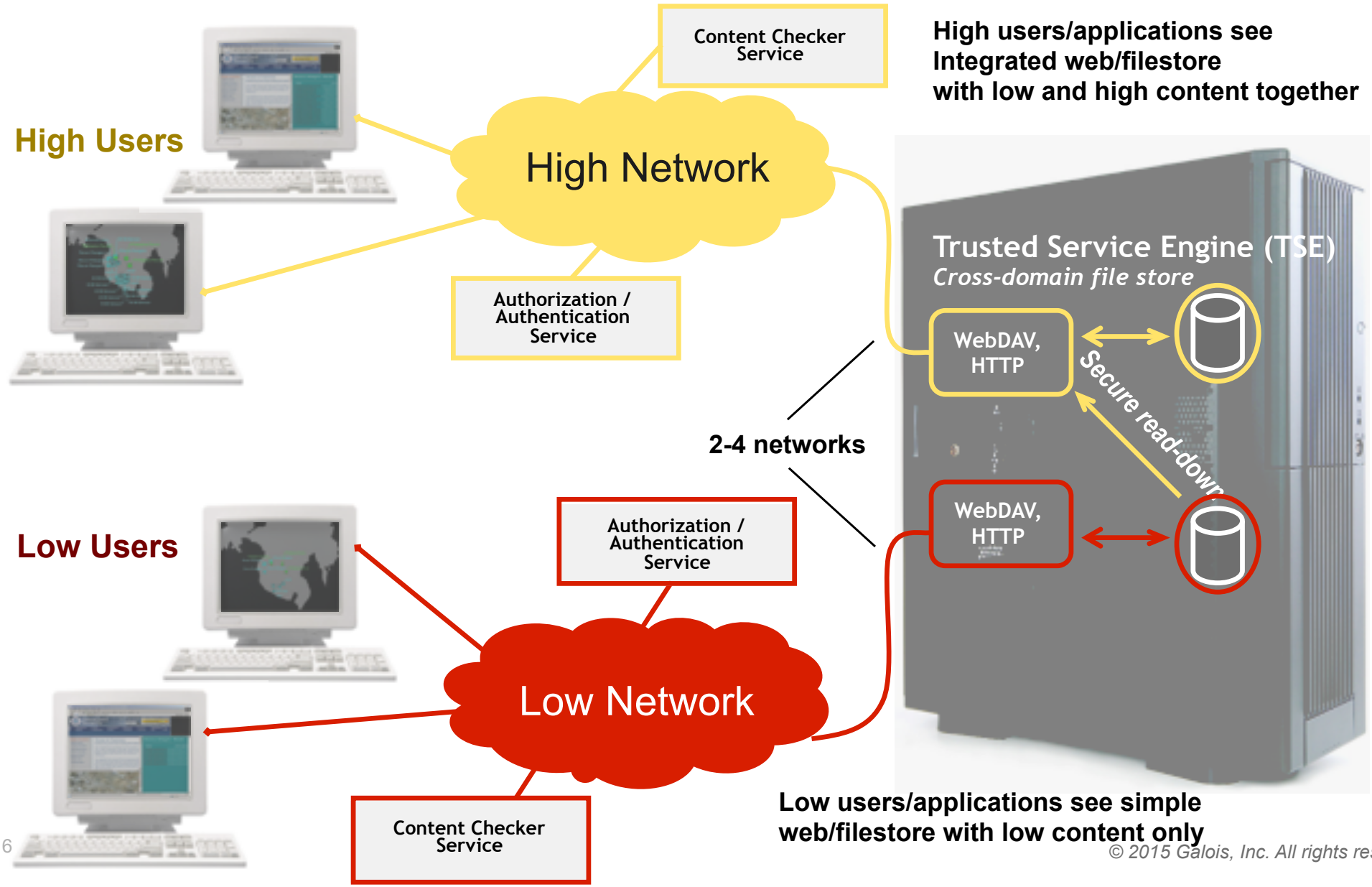
Monolithic OS approach



MILS approach



The Trusted Services Engine (TSE)

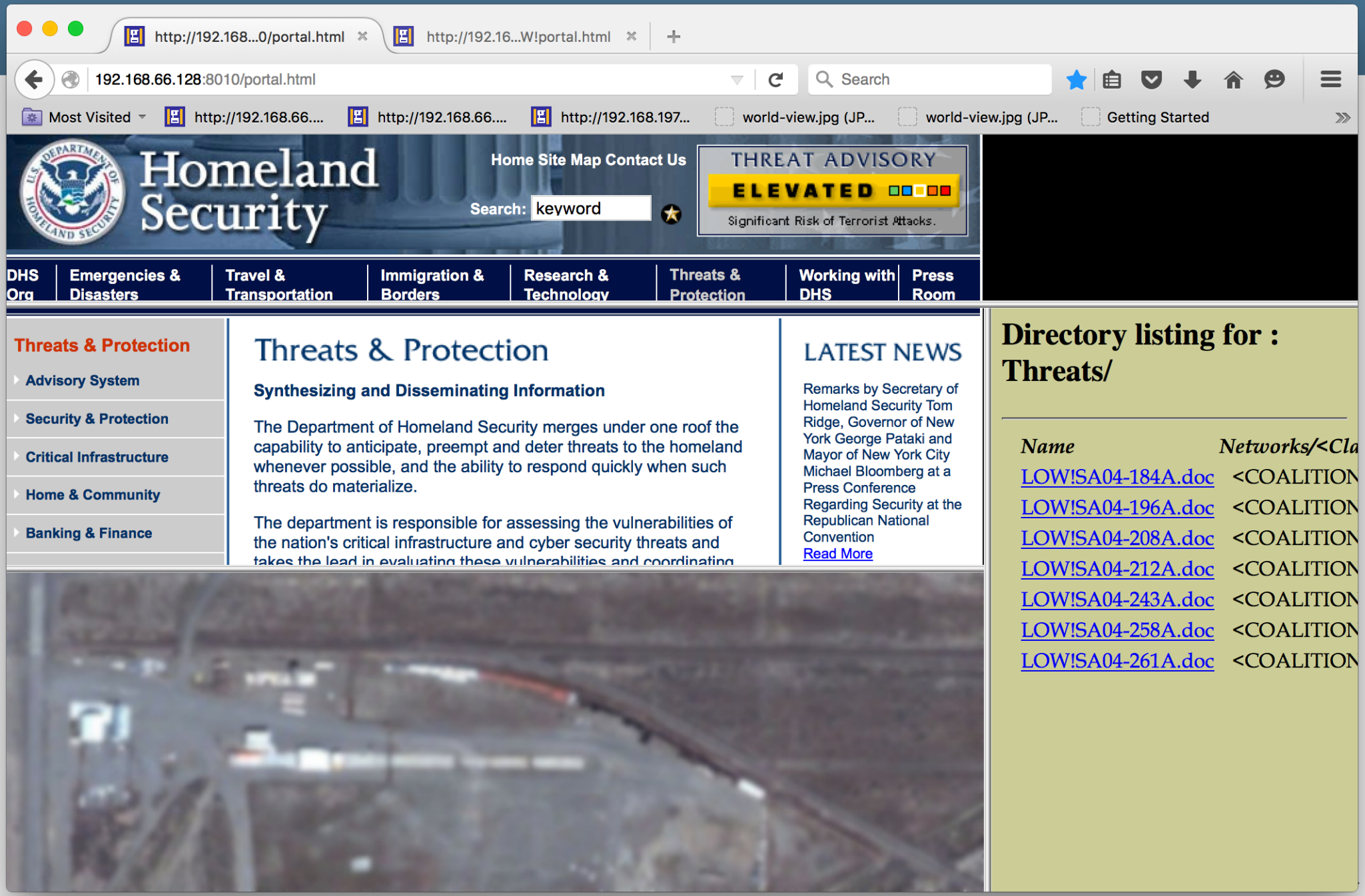


TSE demo

- *breathtaking demo goes here*

| galois |

Low's view of TSE



galois

High's view of TSE

http://192.168...0/portal.html | http://192.16...W!portal.html

192.168.197.128:8010/LOW!portal.html

Search

Most Visited | http://192.168.66.... | http://192.168.66.... | http://192.168.197... | world-view.jpg (JP... | world-view.jpg (JP... | Getting Started

Homeland Security

Home Site Map Contact Us

Search: keyword

THREAT ADVISORY
ELEVATED
Significant Risk of Terrorist Attacks.

DHS Org | Emergencies & Disasters | Travel & Transportation | Immigration & Borders | Research & Technology | Threats & Protection | Working with DHS | Press Room

Threats & Protection

- Advisory System
- Security & Protection
- Critical Infrastructure
- Home & Community
- Banking & Finance
- Health & Safety

Threats & Protection

Synthesizing and Disseminating Information

The Department of Homeland Security merges under one roof the capability to anticipate, preempt and deter threats to the homeland whenever possible, and the ability to respond quickly when such threats do materialize.

The department is responsible for assessing the vulnerabilities of the nation's critical infrastructure and cyber security threats and takes the lead in evaluating these vulnerabilities and coordinating with other federal, state, local, and private entities to ensure the

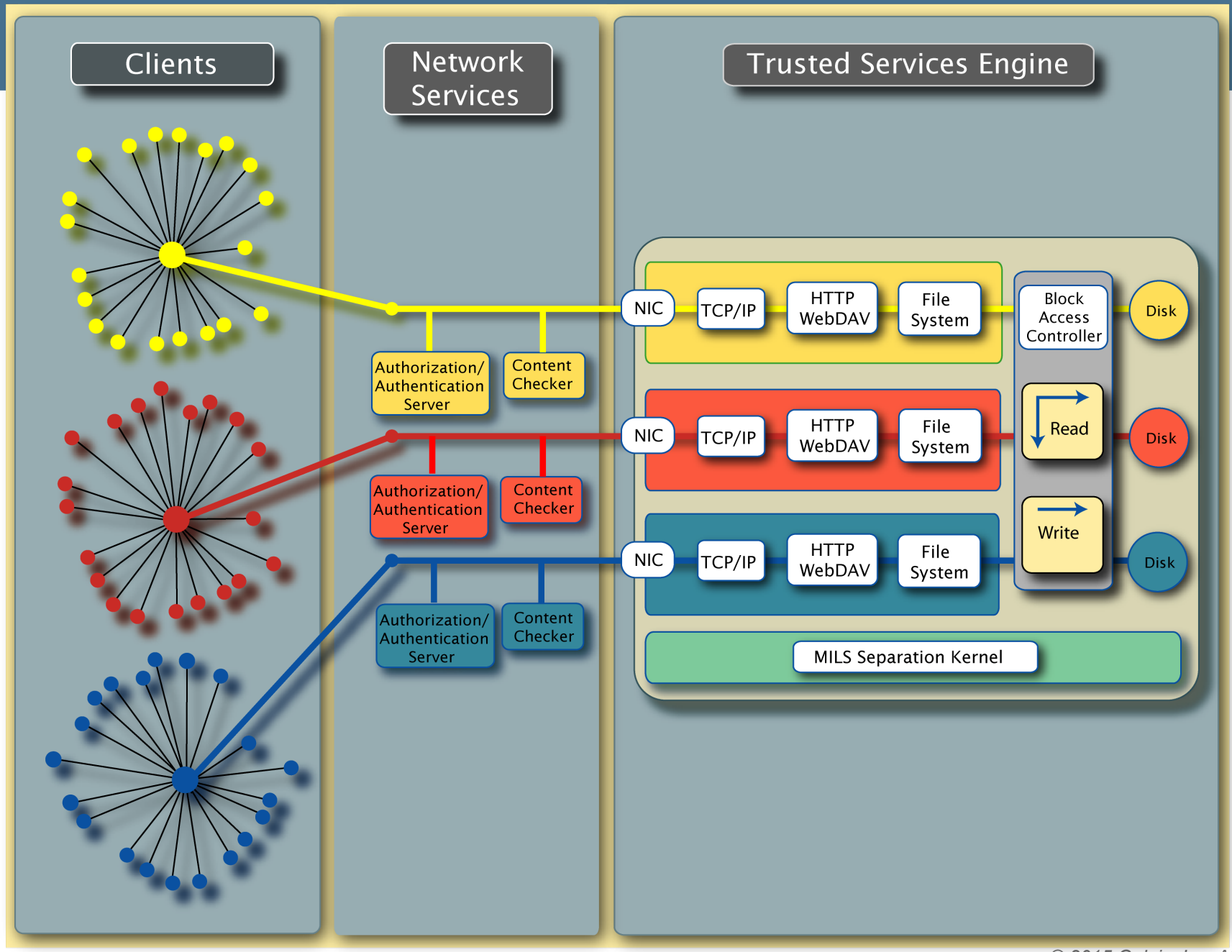
LATEST NEWS

Remarks by Secretary of Homeland Security Tom Ridge, Governor of New York George Pataki and Mayor of New York City Michael Bloomberg at a Press Conference Regarding Security at the Republican National Convention
Read More

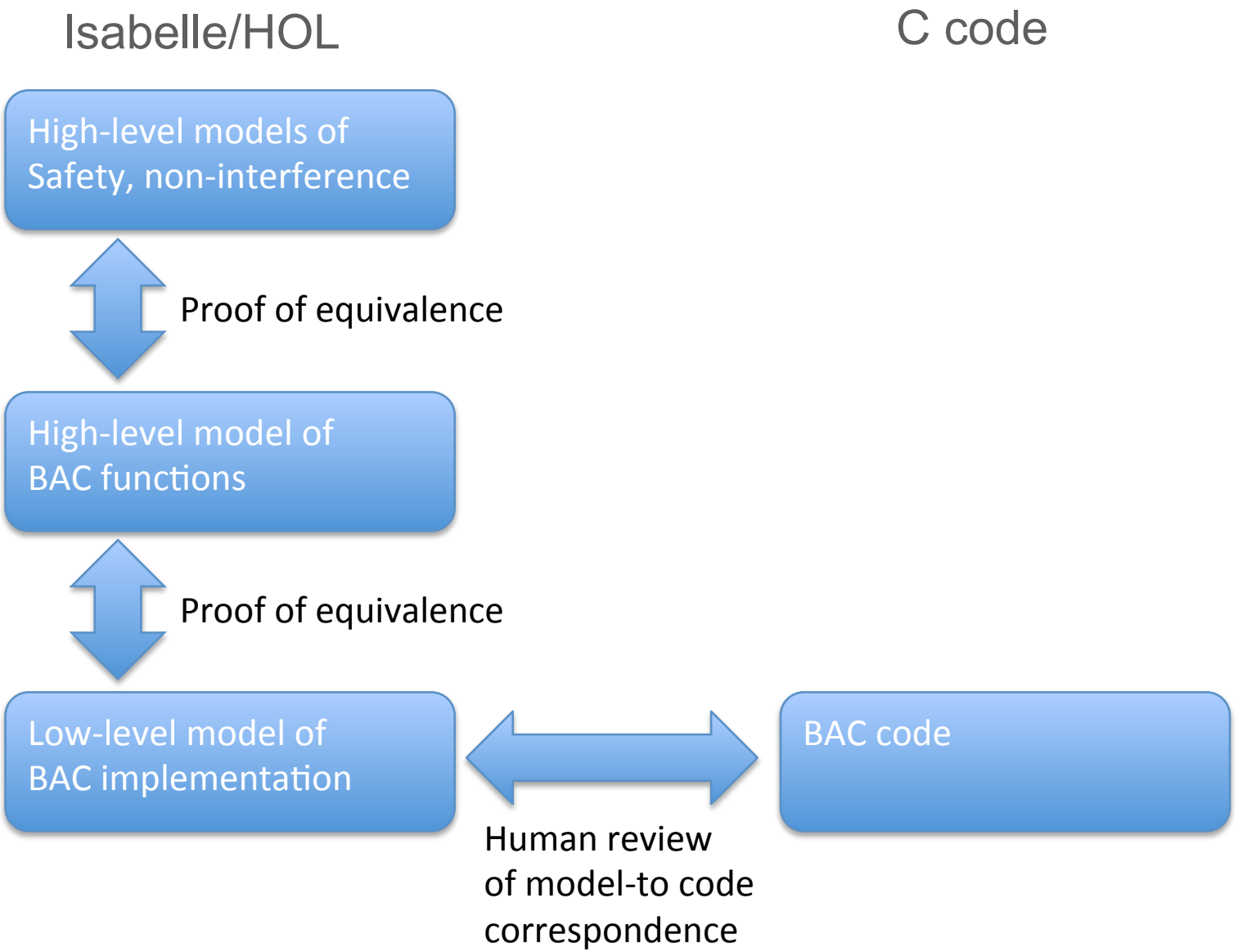
Directory listing for : Threats/

Name	*Networks*
HIGH!SA04-184A-note.doc	<TOP
LOW!SA04-184A.doc	<COALI
LOW!SA04-196A.doc	<COALI
LOW!SA04-208A.doc	<COALI
HIGH!SA04-212A-note.doc	<TOP
LOW!SA04-212A.doc	<COALI
LOW!SA04-243A.doc	<COALI
MEDIUM!SA04-250A.doc	<U
HIGH!SA04-254B-note.doc	<TOP
HIGH!SA04-254C-note.doc	<TOP
HIGH!SA04-254D-note.doc	<TOP
HIGH!SA04-254E-note.doc	<TOP
HIGH!SA04-258A-note.doc	<TOP
LOW!SA04-258A.doc	<COALI

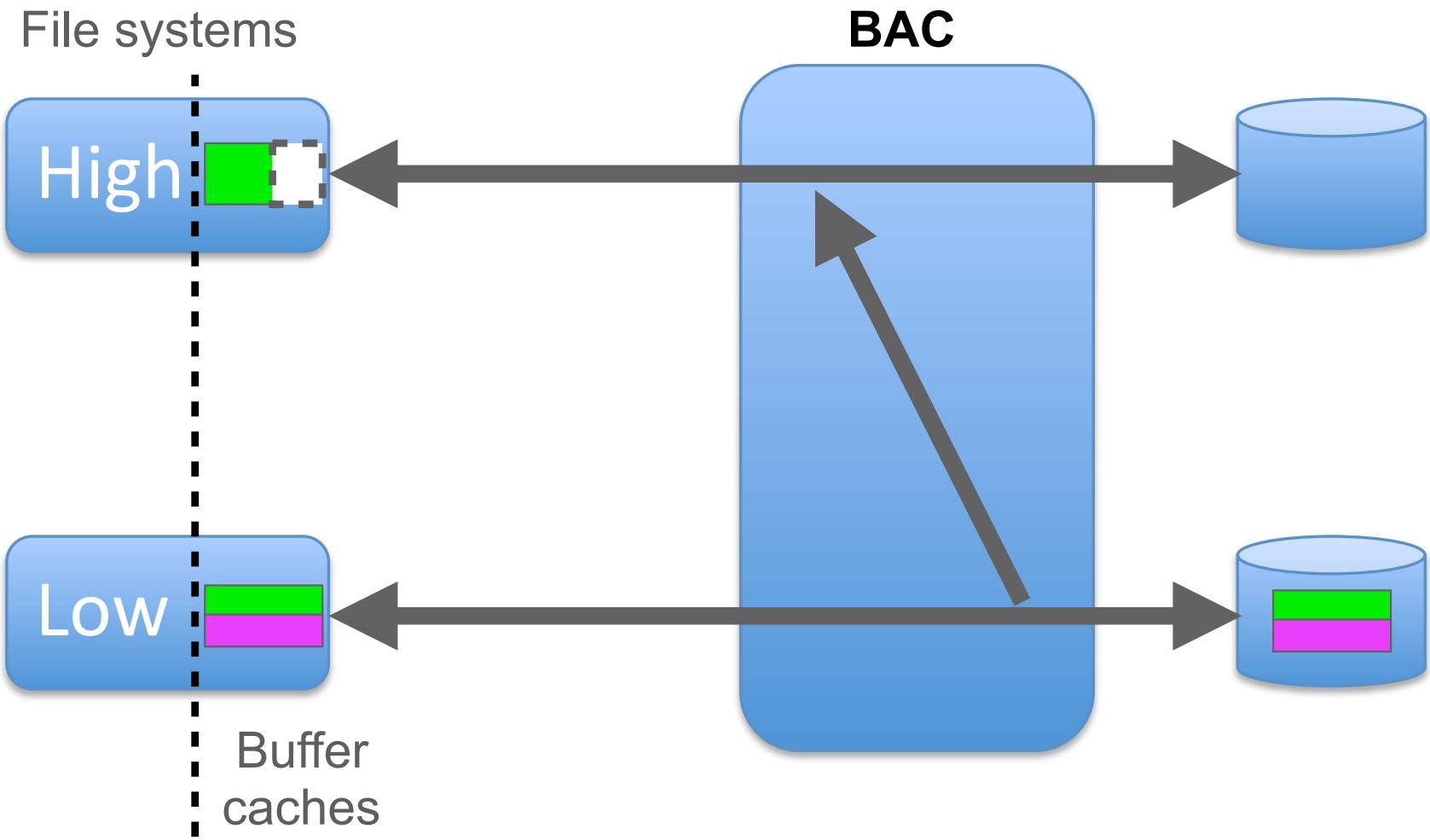
TSE architecture



Block Access Controller assurance



A surprise challenge: consistency across domains



A shifting landscape of software evaluation, certification and accreditation

1985

2005

U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness

Version 1.03

IAD

Information Assurance Directorate

29 June 2007

2009

NIST Special Publication 800-53
Revision 4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2012

U.S. Department of Commerce
John E. Bryson, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

TSE Project

Operating system options

Assurance-level

GENERAL DYNAMICS
C4 Systems

seL4

NICTA

LynxSECURE

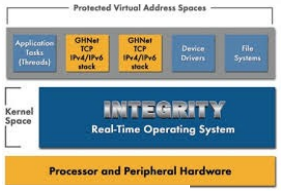
LynxOS 7.0

LynxOS-178

WIND RIVER

GNAT Pro High-Integrity for MILS

Green Hills SOFTWARE



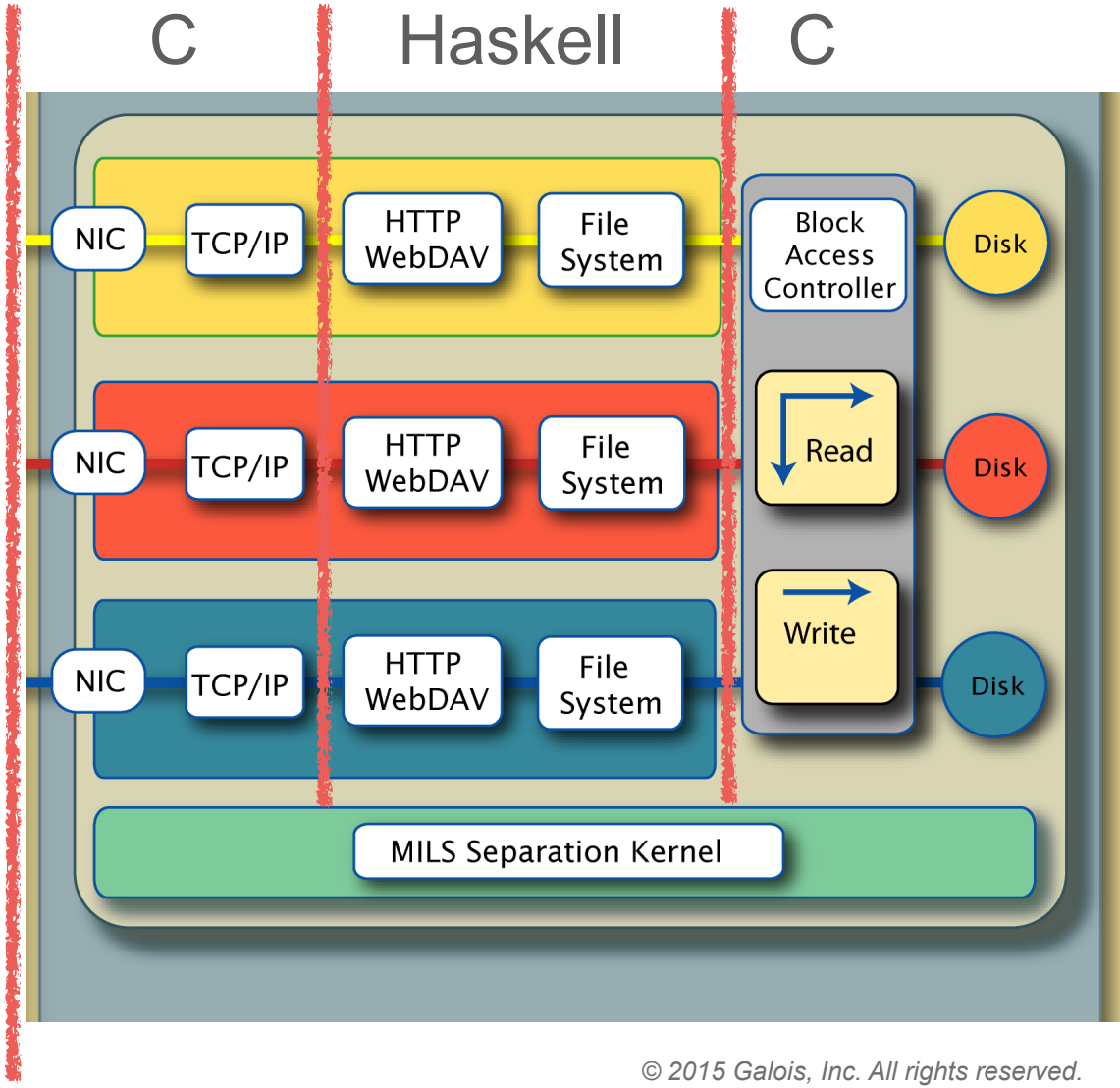
Sun solaris Trusted Extensions COMMON DESKTOP ENVIRONMENT

Time

ORACLE SOLARIS Trusted Extensions Common Desktop Environment

Some lessons we learned

- Implementation language
- Decomposition can surprise
- Theorem proving is hard
- Communication is harder
- Evaluation, certification and accreditation is bewildering



Applying lessons learned

- Tearline wiki
- Federated search
- Separation Kernel SBIR
- Trusted handheld

Applying lessons learned: SMACCMPilot

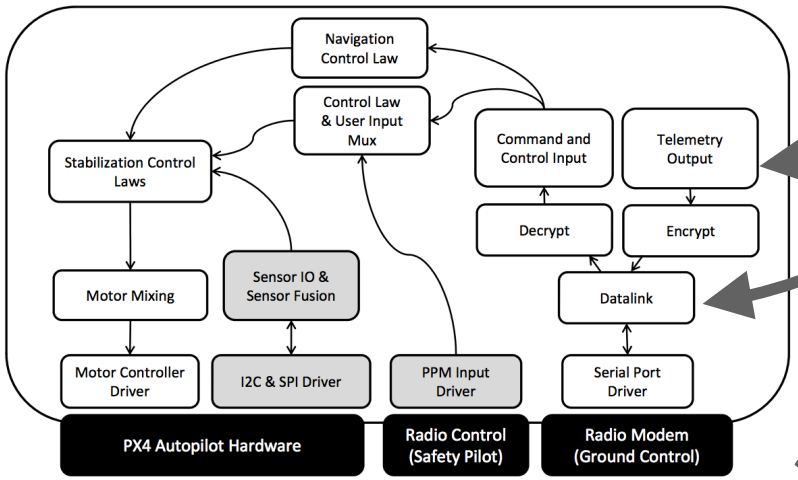
http://www.cbsnews.com/videos/creating-drones-that-cant-be-hacked/

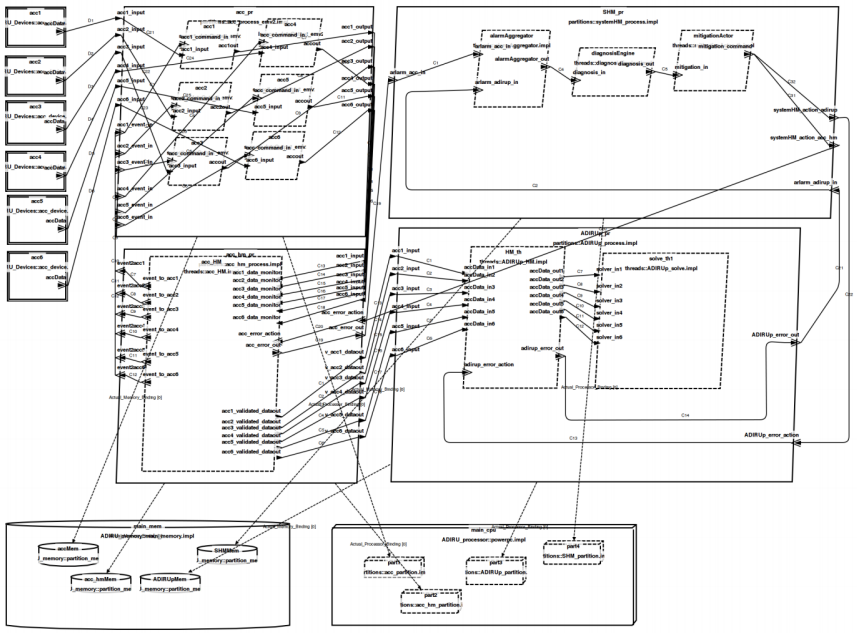
Applying lessons learned: SMACCMPilot

Architecture specification in Tower

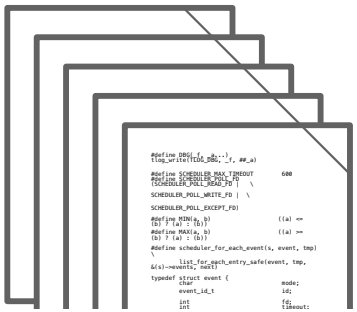
Component specifications in Ivory

Generated AADL model





Generated implementation



Outstanding challenges

- Finding a trustworthy platform to run trusted systems on
  - COTS CPU's are very complex
    - Security mechanisms such as TPMs, IOMMU's, secure enclaves, etc, are important, but *add complexity*
  - trustworthy CPU's are not COTS
  - assurance in the face of multicore is ongoing research
- The market for trustworthy systems is still emerging - *still a hard sell*
  - though the value proposition is (sadly) growing fast
- Complexity is inevitable
  - how to analyze systems with *emergent behavior*

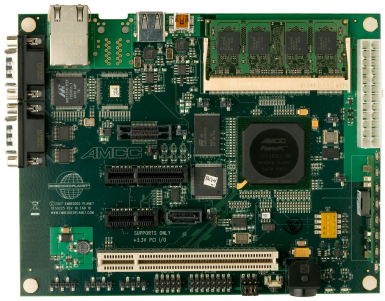
Questions?

dylan@galois.com

Backup slides

A shifting hardware landscape

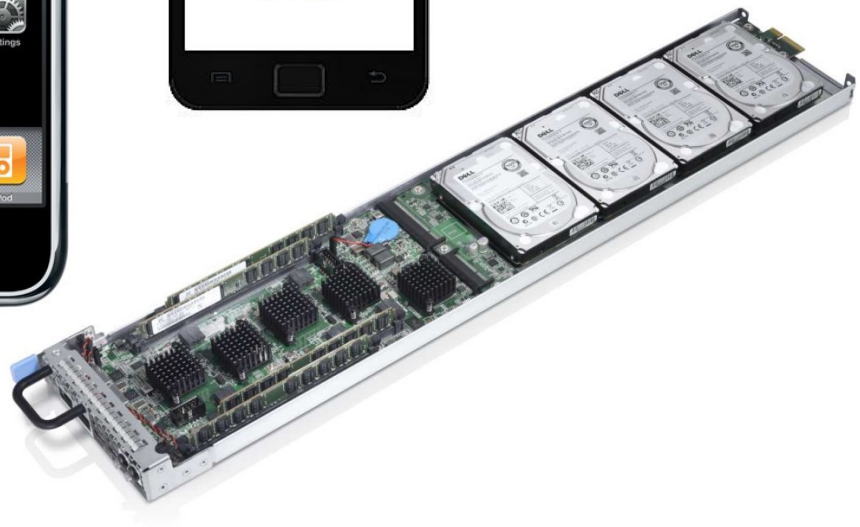
2002



PowerPC

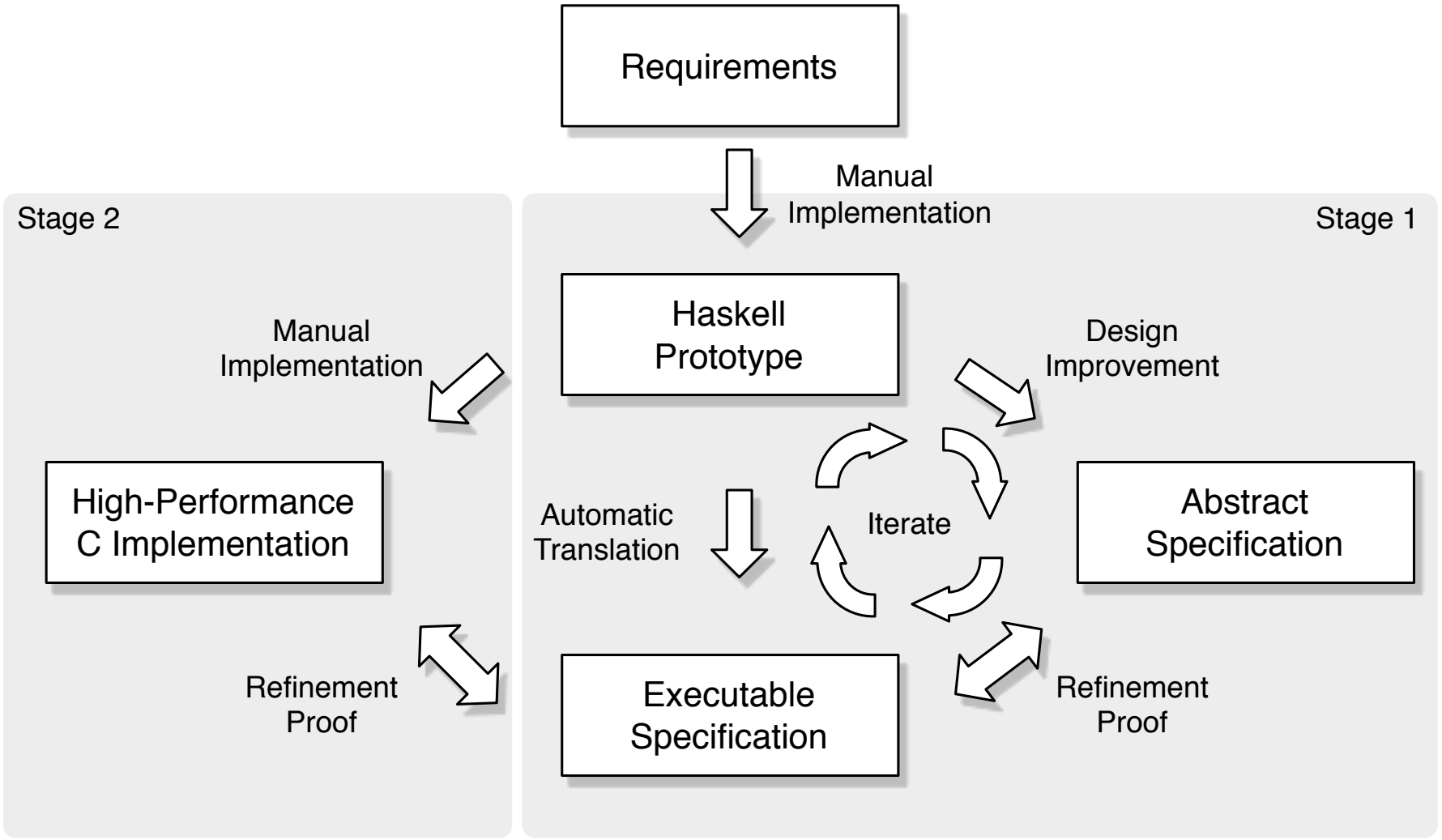
2006

2007



ARM

NICTA's seL4 design process



from "Comprehensive Formal Verification of an OS Microkernel" Klein et al, ACM TOCS Feb 2014

The accreditation process

Enterprise Connection Division (NSC)

DoD Cross Domain Solutions Connection Process Diagram

Phase 1: CDS Categorization and Criticality Determination

- Customer contacts CDSE to discuss requirement and submits required documentation to CDSE
- CDSE reviews required documentation, registers the requirement in SGS and conducts an Operational Impact assessment. For VLoR the CDSE conducts a VLoR assessment. Once completed, the CDSE submits a CDTAB agenda request to the CDTAB Secretariat
- **CDTAB** Determines if a CDS is required, categorizes CDS, recommends technology and for VLoR conducts risk review
- **DSAWG** Reviews CDTAB determination and authorizes related way ahead for the CDS
- If approved by DSAWG, the CDS Team issues a ticket number and moves the ticket to the respective phase based on the CDS Categorization

Phase 2: CDS Engineering, Security Control Selection, and Security Control Implementaion

- Customer works with CDSE to engineer CDS, complete and upload Phase 2 CDA, ST&E Plan and Procedures to SGS.
- CDSE conducts a risk assessment based upon the relevant security controls based upon the CDS Categorization (RDAC, VLOR, etc) For RDAC a CDSE will request a GCT assessment from the CDTAB Secretariat. Once a draft risk assessment is completed the CDSE submits a CDTAB agenda request
- **CDTAB** Concurs or non concurs with risk rating
- **DSAWG** Authorizes Issuance of a CDSA for ST&E and sometimes continued operational use upon ST&E result review by CDSE
- If approved by DSAWG, the CDS Team issues a CDSA for ST&E

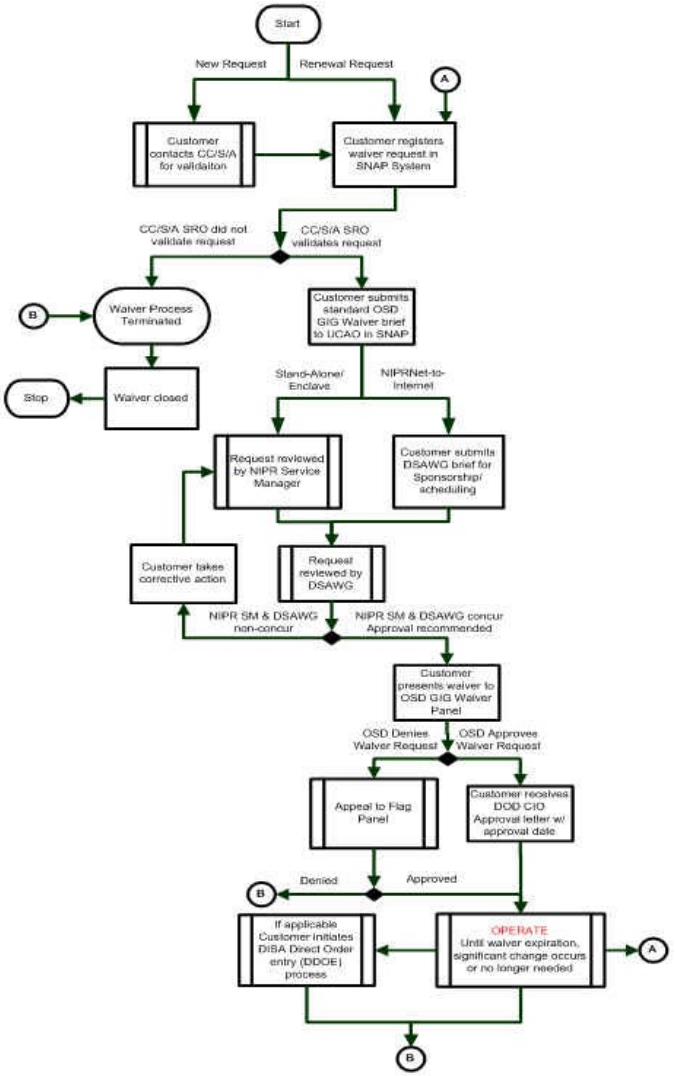
Phase 3: CDS Security Control Assessment and Authorization

- ST&E is completed and the customer submits a Phase 3 CDA and ST&E results to the CDSE.
- CDSA reviews the ST&E results and verifies that they are in accordance with the ST&E plan. If the results differ from the plan CDSE may adjust the previous risk assessment and return to CDTAB and DSAWG with that assessment. If the ST&E results are in accordance with the ST&E plan the CDSA will request a CDSA to be issued from the CDTAB Secretariat. .
- **CDTAB** Concurs or non concurs with risk rating
- **DSAWG** Authorizes Issuance of a CDSA for Operational Use
- If approved by DSAWG, the CDS Team issues a CDSA for Operational use

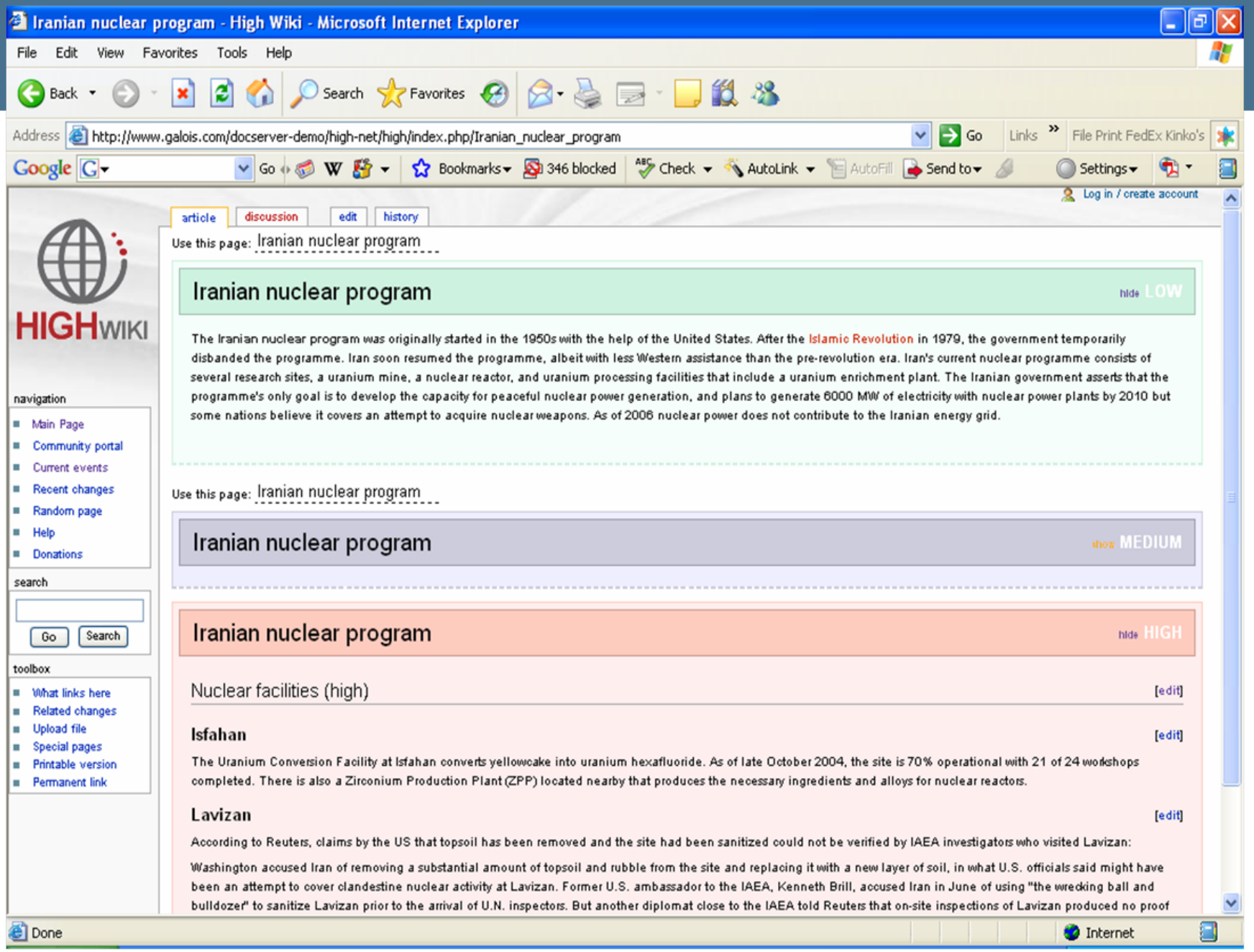
Phase 4: Operational CDS Monitoring

- Customer submits annual revalidation memo to CDSE. CDSE uploads to SGS.
- CDSE forwards a request for an annual review to the CDTAB Secretariat. If the DSAWG approval has also expired the item will be reviewed by CDTAB and DSAWG prior to CDSA issuance
- **CDTAB** Reviews risk and revalidation requirements
- **DSAWG** Authorizes Issuance of a CDSA for Operational Use
- If approved by DSAWG, the CDS Team issues a CDSA for Operational use

DISA

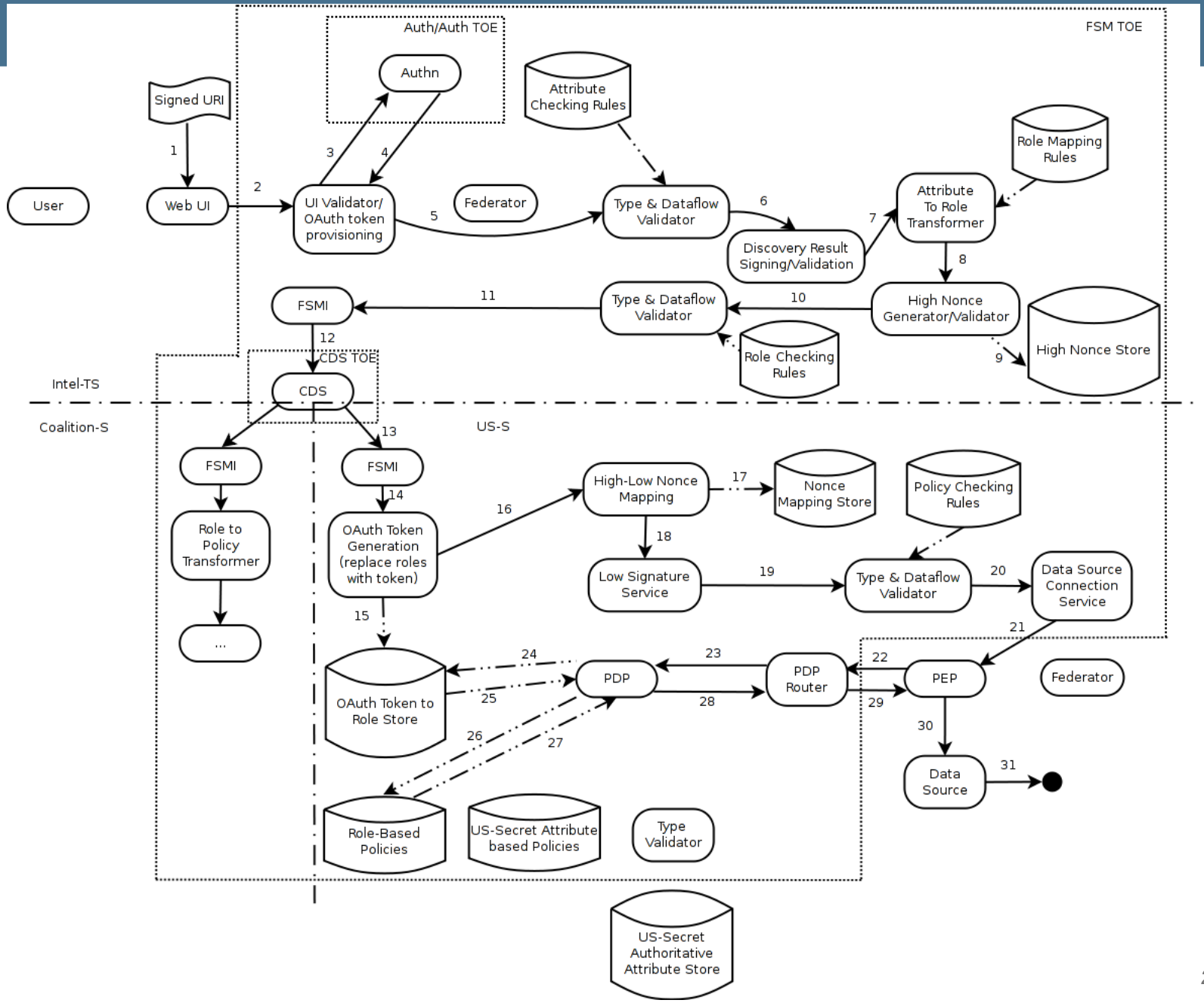


Tearline wiki



galois

Federated search



Trusted handheld project