galois

Cross Domain Solutions
Trusted Web Service Engine

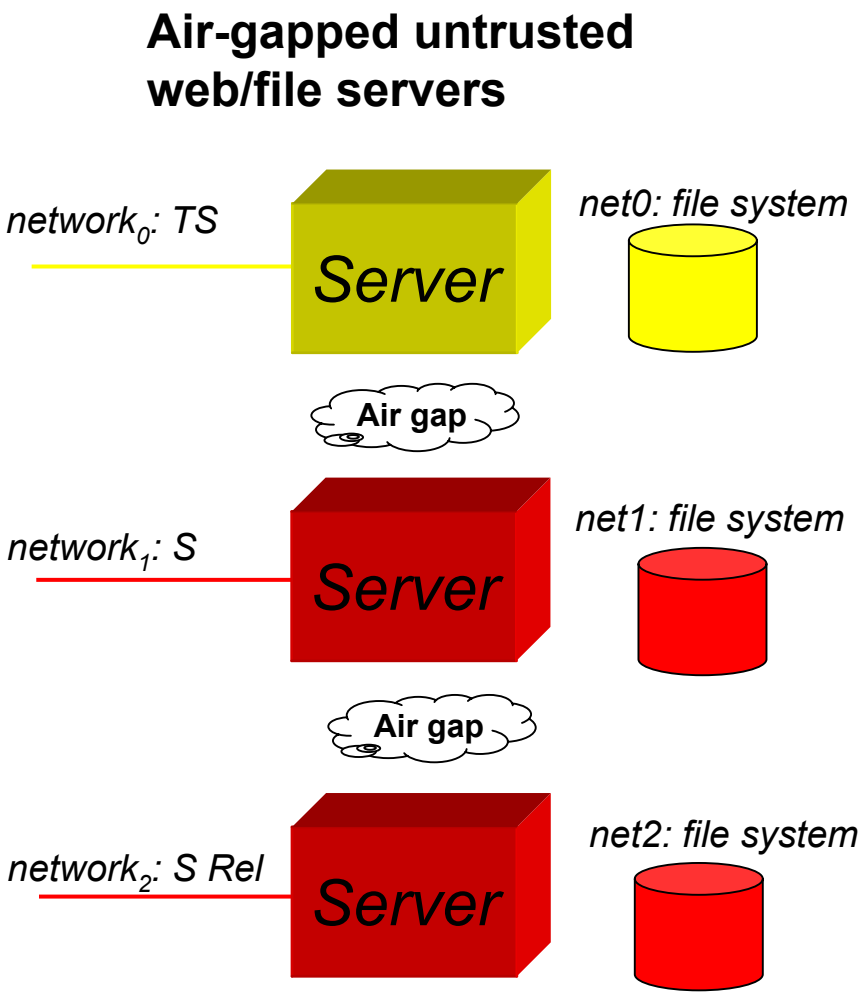
April 2004

John Launchbury
Galois Connections
john@galois.com

Outline

- **The problem**
  - Cross-domain applications require spanning multiple networks, coalition interoperability
  - GIG, ForceNet, JC2 require multi-level security processing
- **The solution**
  - Preserve the same high assurance as the air gap
  - Enable new functionality with a multi-level web server
- **The applications**
  - Cross domain solutions enabled by the trusted web server
- **The approach**
  - Multiple Independent Levels of Security (MILS) architecture plus additional formal methods

Separation Implemented via "Air-gaps"



Problems

Expensive and limiting

Solution doesn't scale

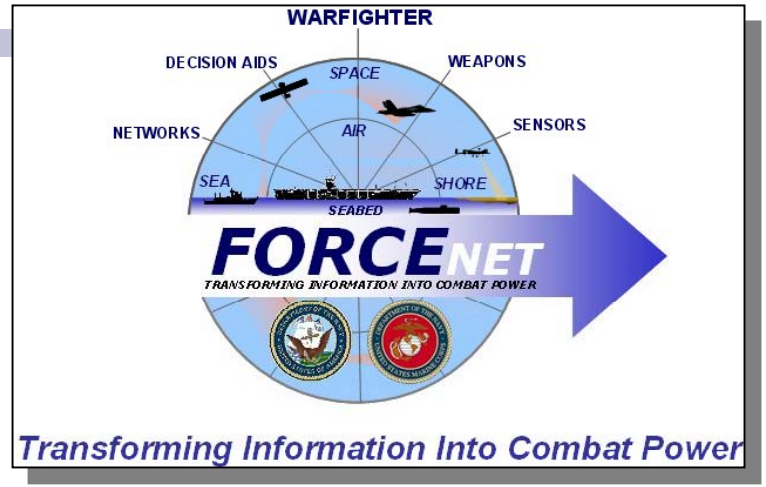
Problems Of Air-gapped Networks

- **Lack of access**
  - Innocuous `Low` information created, for convenience, on `High` network, and (implicitly) labeled as `High`
- **Too many networks**
  - Each distinct level needs separate infrastructure
  - Excessive space, weight and power (SWAP)
- **Inaccurate labeling**
  - Many security levels are collapsed into that of the available network
- **Inaccurate clearance**
  - Existing network “reused” in new setting, e.g. SIPRNET (`S/NOFORN`) used to carry `S/REL` traffic in Afghanistan
- **Duplication of documents across levels**
  - Version control: changes are not tracked, documents get out of date

… and so on

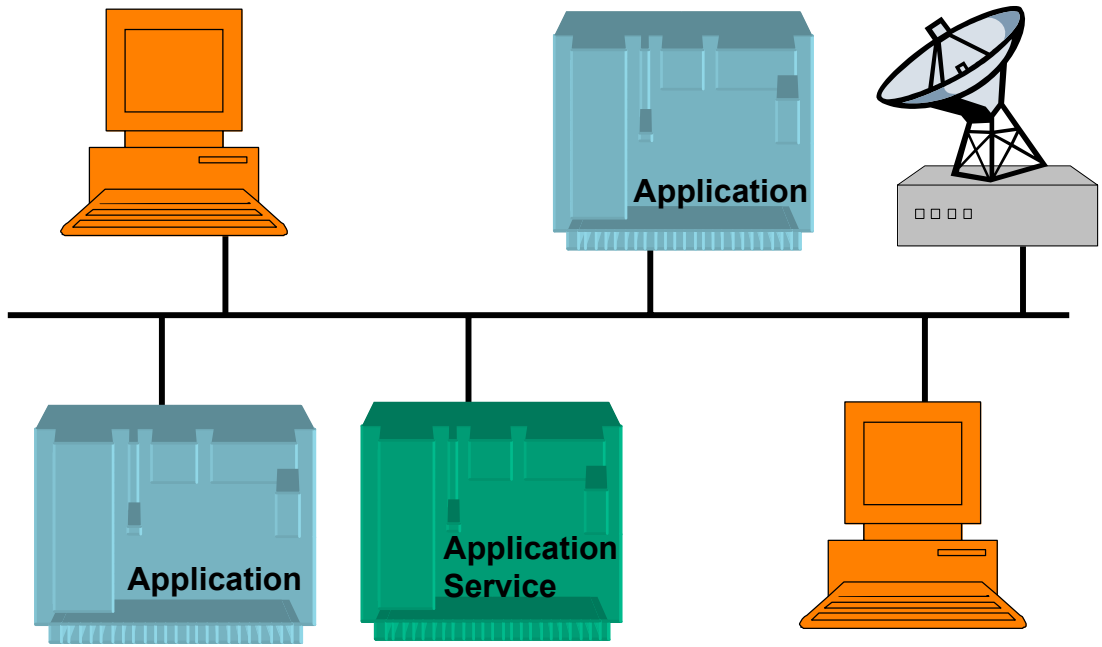
DoD/Navy Context

- Net Centric
- Web Services
- Interoperable
- Composeable
- Distributed
- Secure
- Adaptive

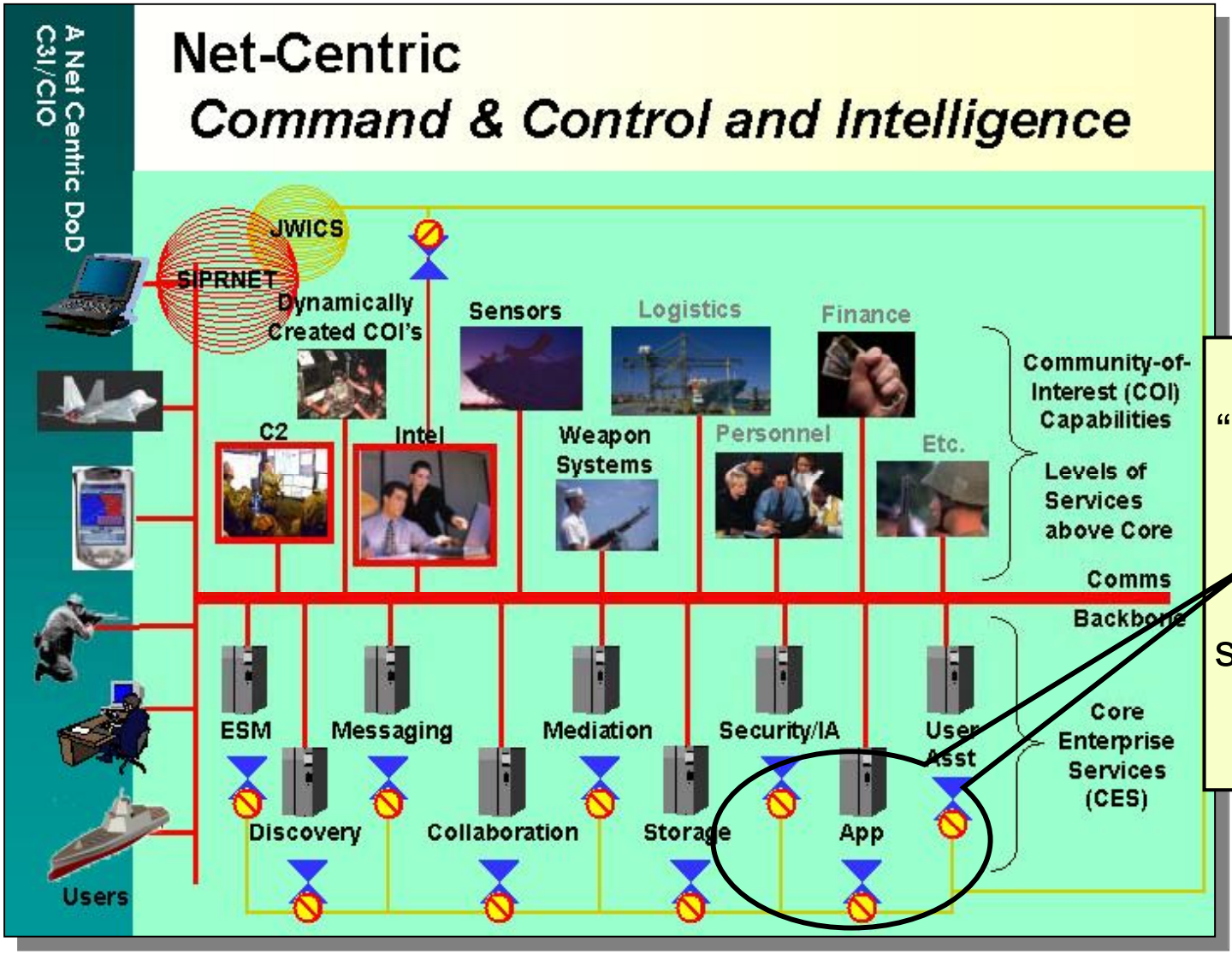


Layered Applications

- Visualization
- Application
- Domain Specific Application Services
- Domain Specific Data Services

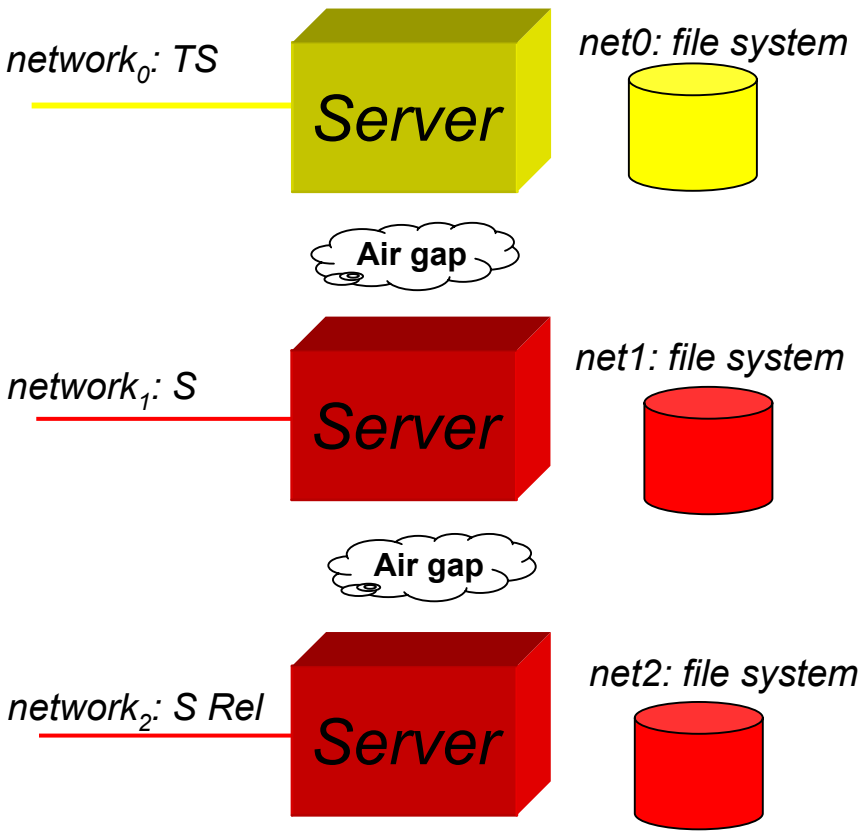


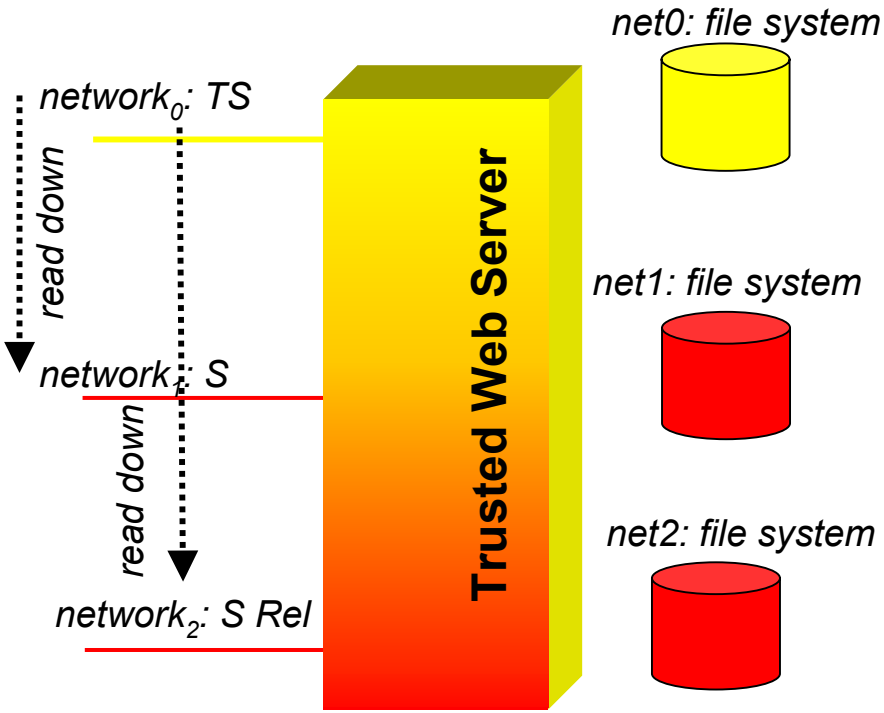
FORCEnet Architecture



Many smart "data-diodes"- Information flow across multiple security levels

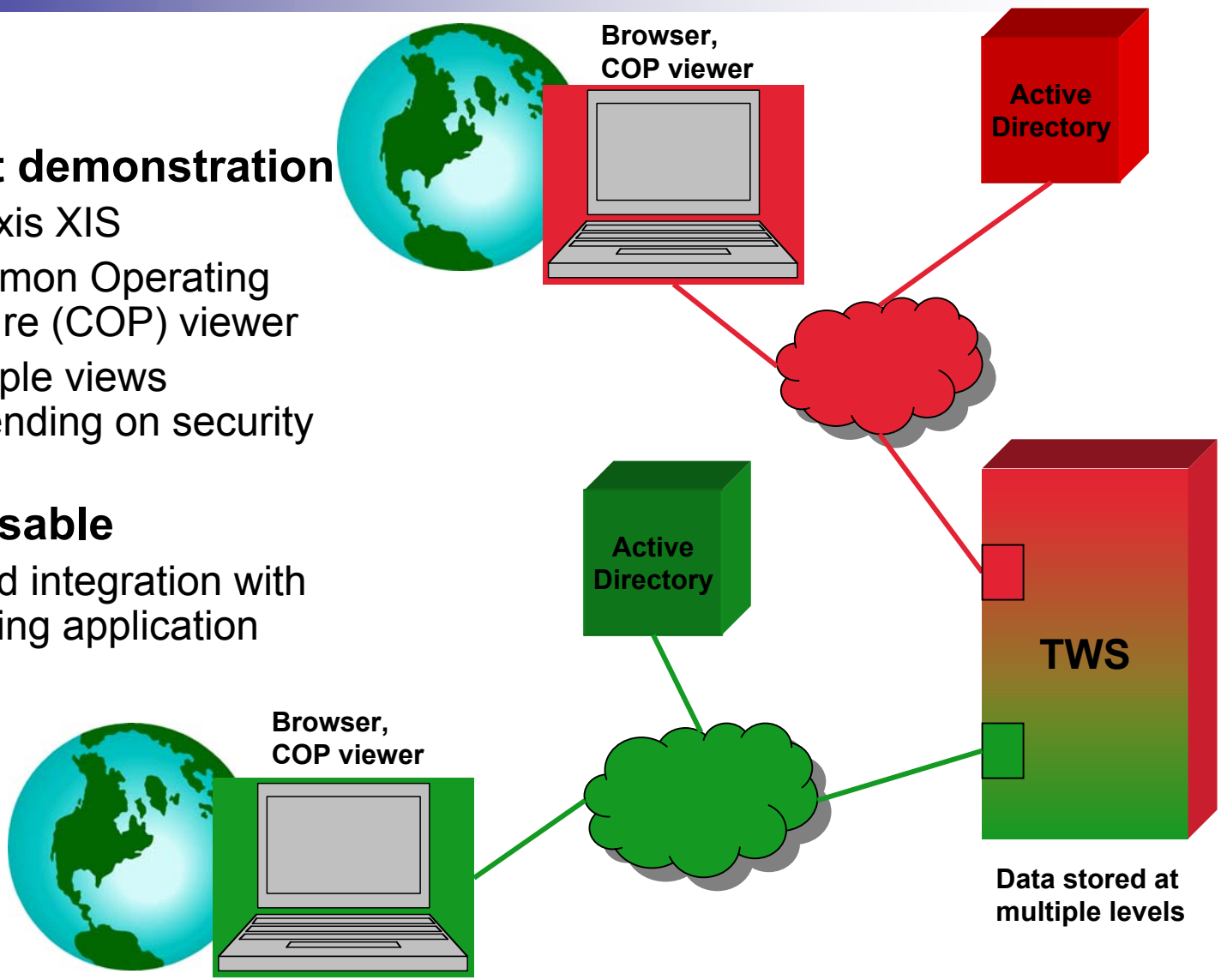
Solution: Replace The Air-gap With High Assurance Of Separation



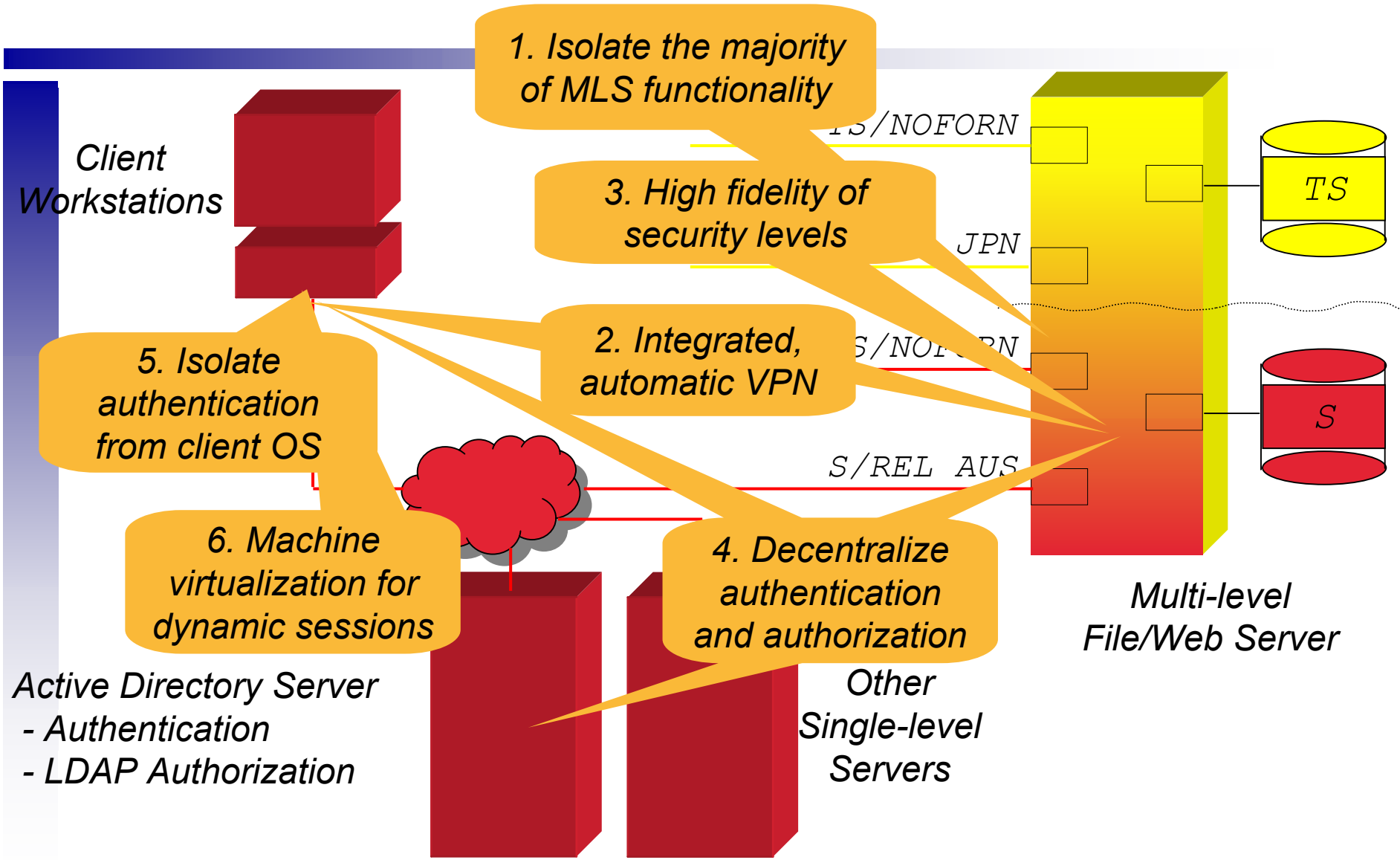


Composing With Existing Applications

- **Current demonstration**
  - Polexis XIS
  - Common Operating Picture (COP) viewer
  - Multiple views depending on security level
- **Composable**
  - Rapid integration with existing application



Architectural Principles



Security Assurance Requirements Driven by Threat Level and Information Value

THREAT LEVEL	
T1	inadvertent or accidental events
T5	Sophisticated adversary with moderate resources who is willing to take significant risk (e.g. international terrorists)
T7	Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g. nation-states in time of crisis)

INFORMATION VALUE	
V1	negligible adverse effects or consequences
V4	serious damage to the security, safety, financial posture, or infrastructure…
V5	exceptionally grave damage to the security, safety, financial posture, or infrastructure…

Assurance at V4/T7, V5/T5 require EAL 6**…**

(excerpted from IATF Release 3.1)

High Level Features Of The Solution

- **Non-interference between networks**
  - With very high assurance
- **Separation between security levels within a network**
  - With high assurance
- **Reduce Space, Weight, and Power**
  - Reduce duplication across networks
- **Maintain the user's current view of the network**
  - Ease of use and administration
  - Do not require new training of network users
  - Use existing COTS workstations
- **Provide additional access**
  - Appropriate access of documents between networks (read-down)
  - Authentication and authorization of access to documents within and between networks
  - Security policies within a network and between networks

Coarse And Fine Grained Assurance

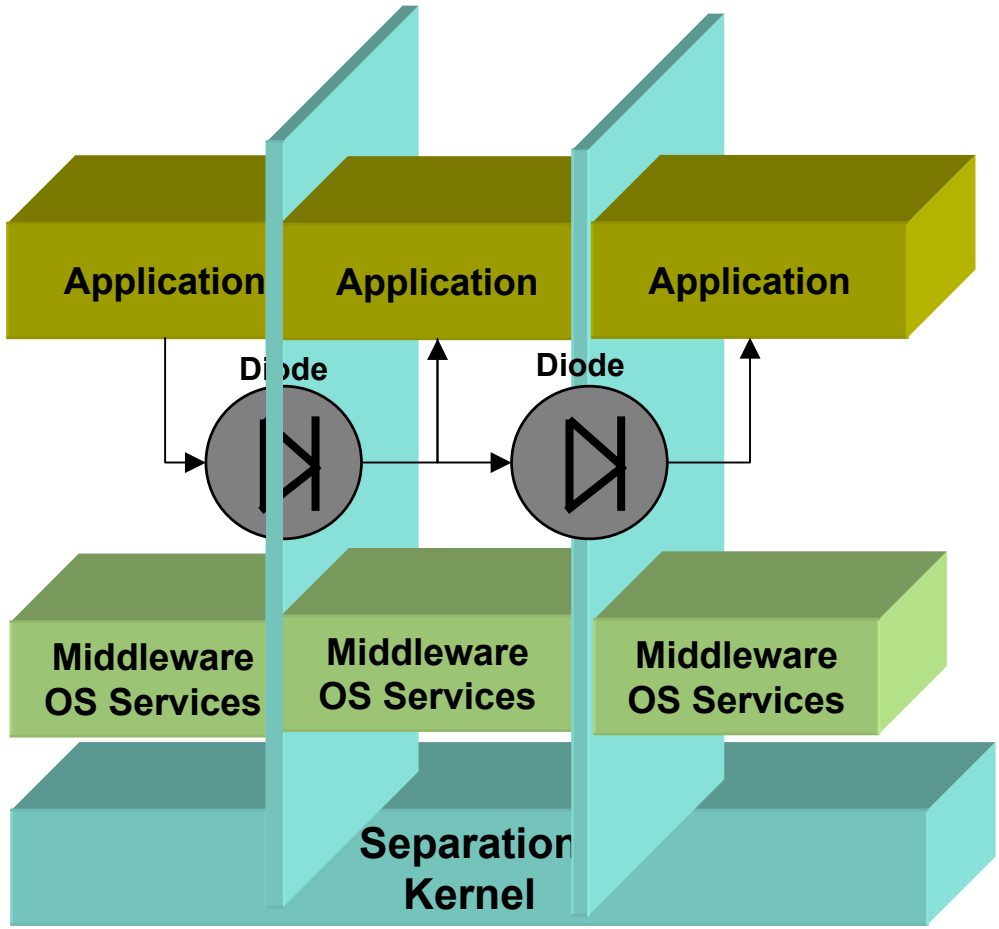
- **Coarse grained policy assurance is extremely high**
  - Requirement
    - No covert storage channels across networks
    - Limited covert timing channels across networks
  - Methods: Formal methods, proof that read-downs do not introduce cross network interference
- **Fine grained assurance is high, but lower than the coarse grained policy**
  - Requirement
    - No unauthorized access to files
    - The web server does not increase storage and timing channels already available within the network
    - Note: Timing, Denial of Service, and traffic analysis threats are available within a network, before the trusted web server is installed
  - Methods: Formal policy, semi-formal design and test

Low Level Features Of The Solution

- **From the point of view of a user**
  - Protocols
    - Web pages (HTTPS)
    - Filestore (WebDAV)
      - Accessible as web-drive
  - URLs still behave as expected
    - When a path identifies a directory, extending the path identifies a member of that directory
    - A URL is still “universal” — it refers uniquely to an object
    - URL format is unmodified for files the user could access before the trusted web server was installed
    - A user can restrict who gets access beyond the security level restrictions

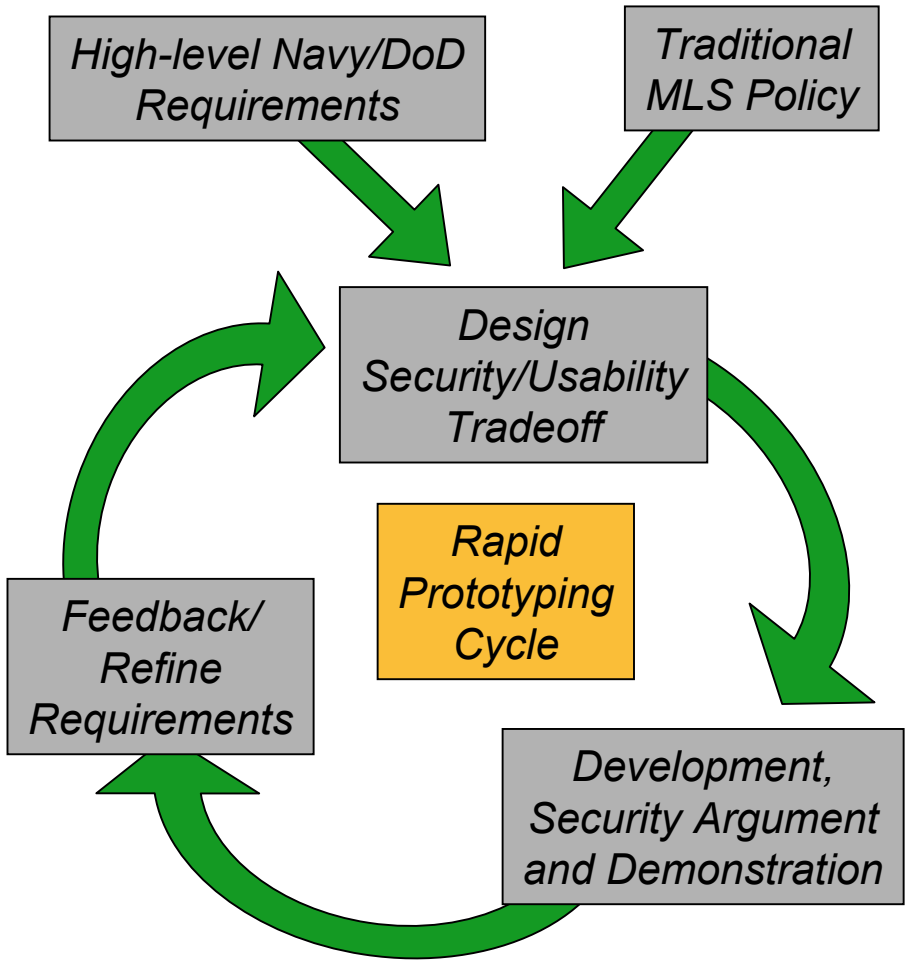
The Approach

- **MILS architecture**
  - High assurance separation kernel at its heart
  - Coarse grained separation mapped onto the kernel
  - Fine grained separation specified and implemented with semi-formal methods
- **Fundamental philosophy**
  - Modularize, according to properties
  - Each component has one function, which it does well
  - Put application security in the application (not in the OS)

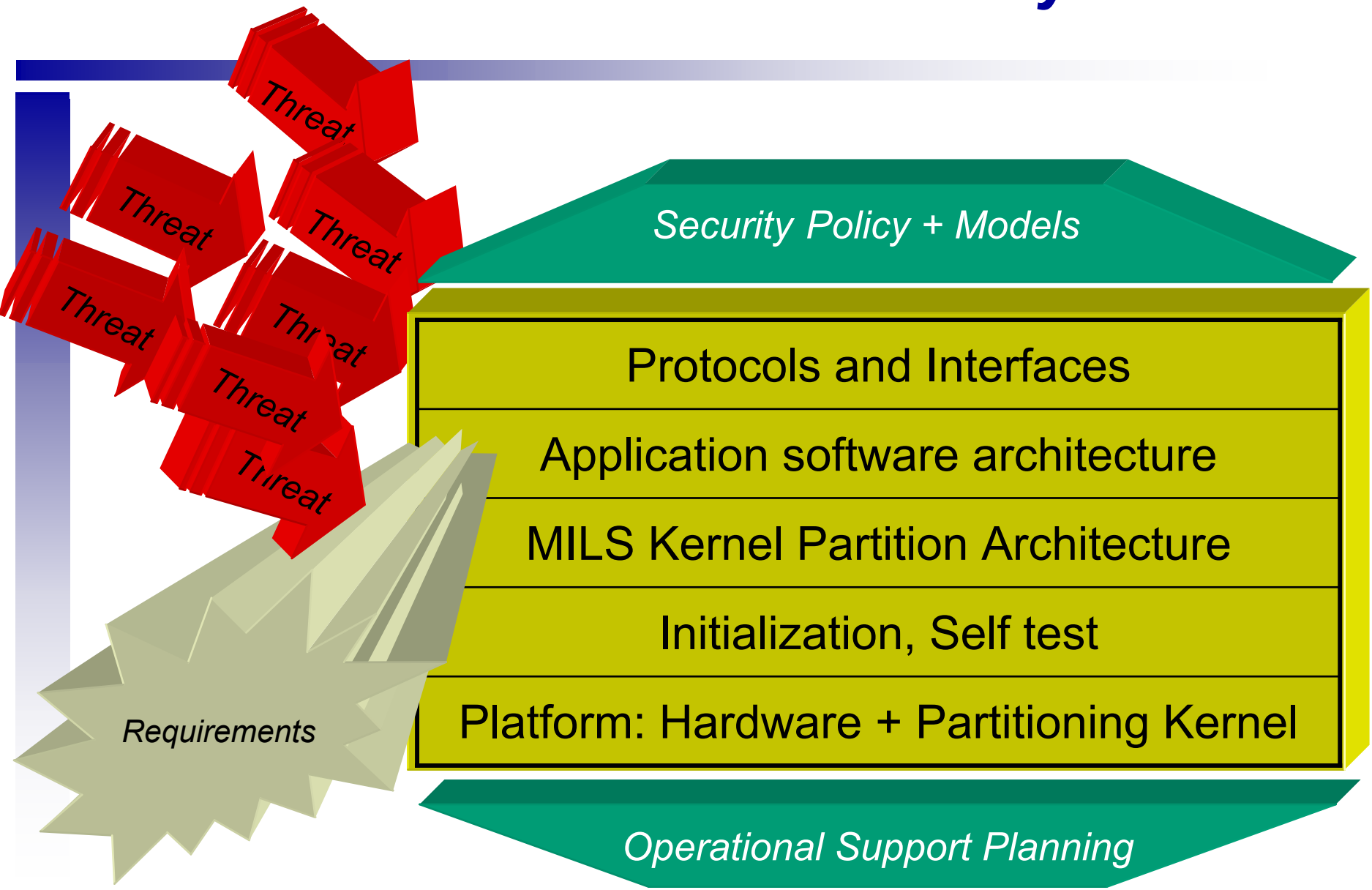


Development Process

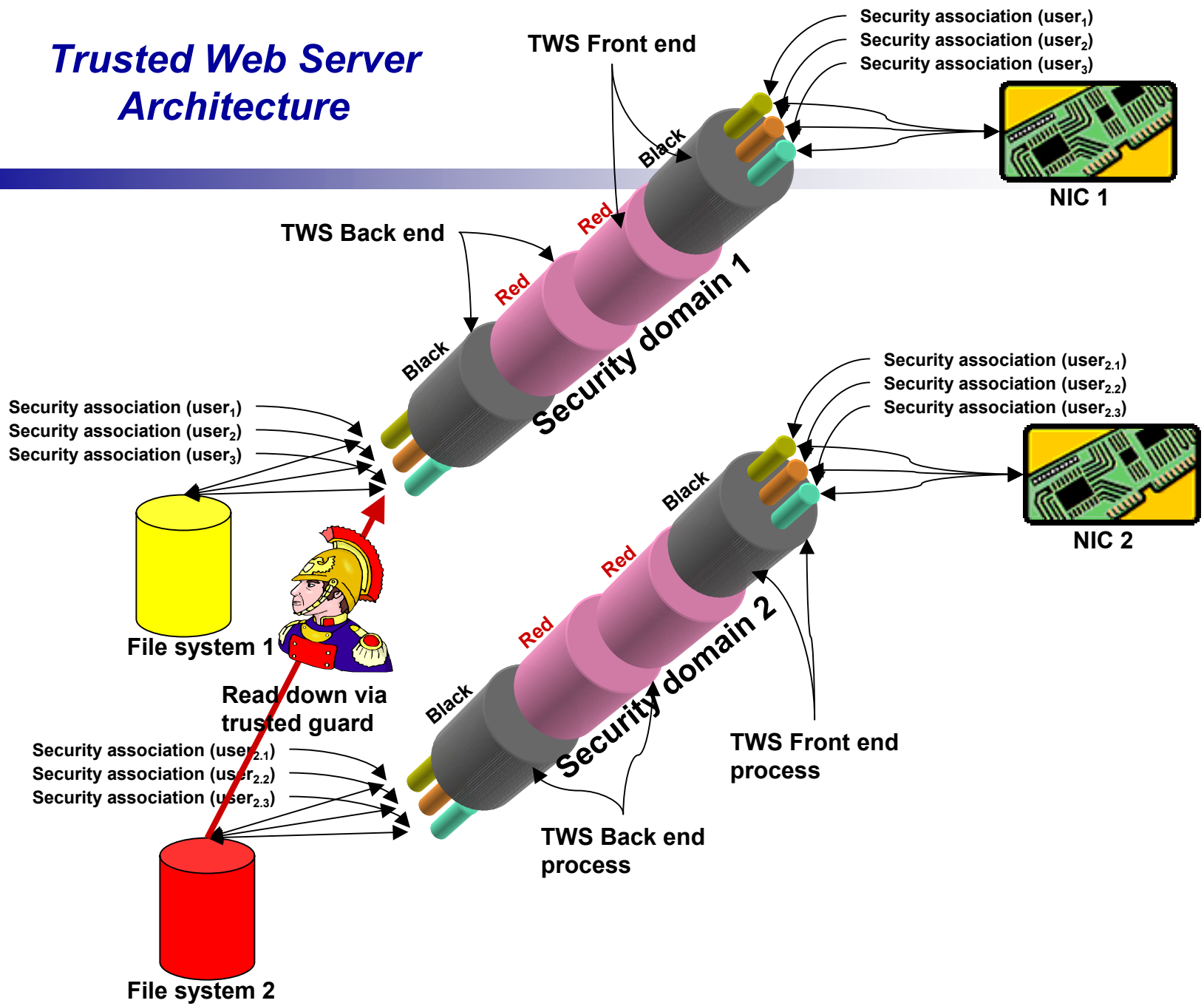
- **Responsive to**
  - Developing requirements
  - Emerging solutions in CDS
  - C&A feedback
- **Development process**
  - Interactive
  - Iterative
- **Prototypes**
  - Elicit requirements from users
  - Test and prove concepts
- **Formal and semi-formal methods**
  - Maintain security argument



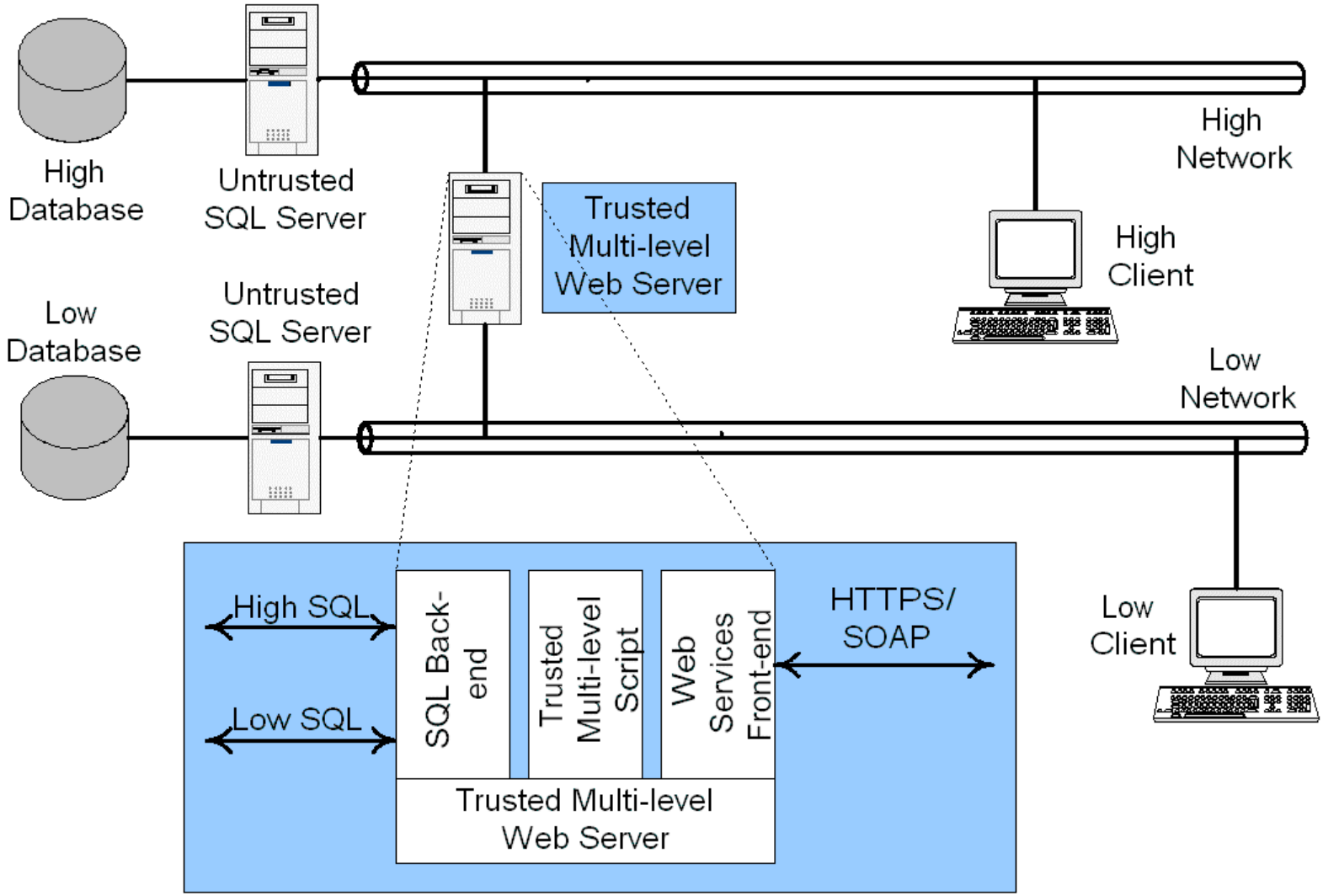
Web Server Abstraction Layers



Trusted Web Server Architecture



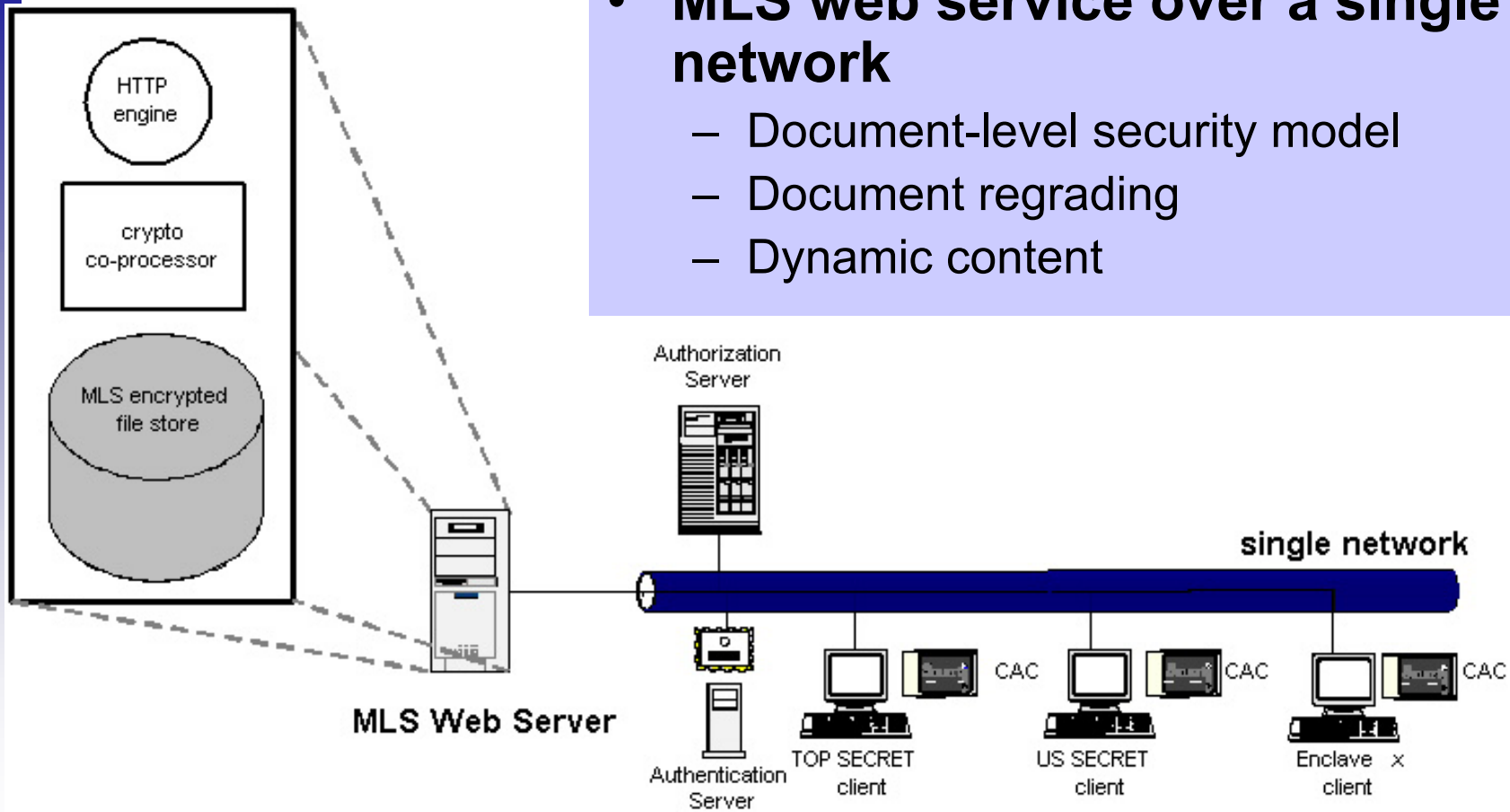
Beyond a Trusted Web Server: Trusted Service Engine



Single-level common operating picture application is served multi-level data drawn from multiple single-level databases

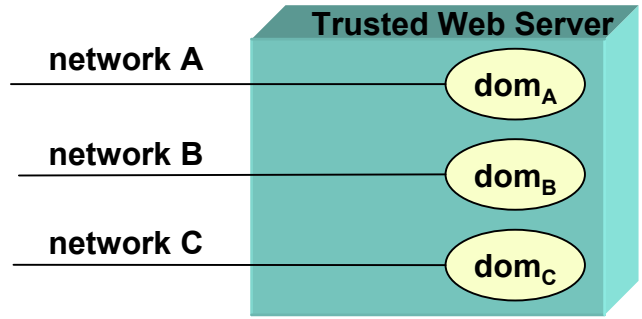
Long Term Vision

- **MLS web service over a single network**
  - Document-level security model
  - Document regrading
  - Dynamic content

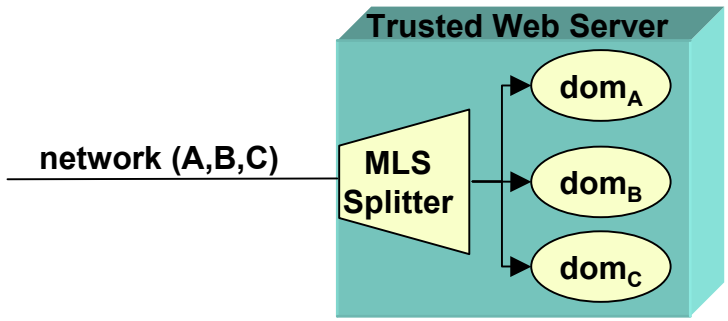


Trusted Server Is An Evolutionary Step Towards The GIG

- Can connect existing networks in support of the GIG vision
- Provides growth path to more than three networks
- Can continue to support networks after they are combined
- Designed to support other internal components, e.g. a regrader



Now: separate networks

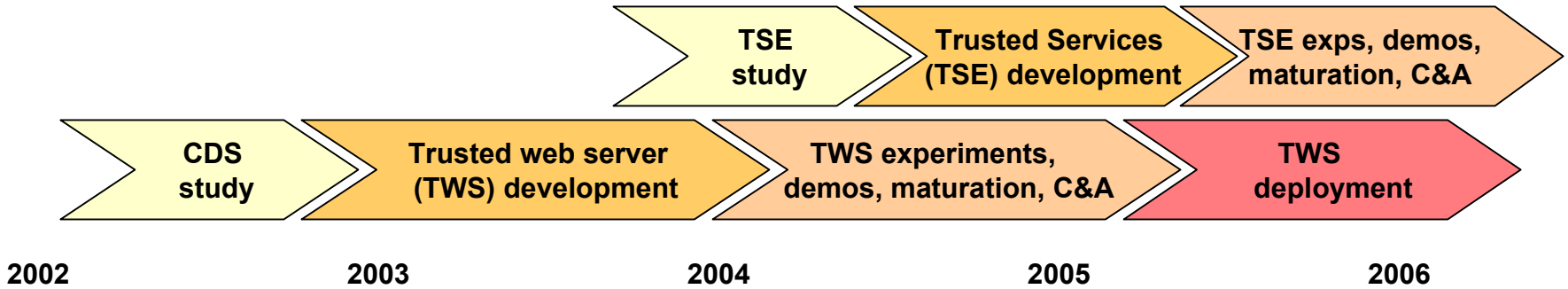


Future: Network collapsed, then split by MLS component

Other Multi-Level Services

- **Email server**
  - Function 1. act as a file store for local user mailboxes
    - IMAP is yet another remote file system protocol
  - Function 2. act as a forwarding agent for remote mail
    - Complicated: Failure, retries, rules, filtering, address rewriting…
- **Multi-level chat**
  - Cross-coalition communication
- **Multi-level documents**
  - Can .doc or .ppt be made multi-level without relying on the virtues of the Microsoft code-base?
- **Machine-machine access**
  - Automatic regrading of COP tracks
  - Automatic reformatting of data

Notional Timeline



- **Core functionality**
  - Trusted web server (TWS)
  - Cross-domain https and WebDAV
- **Extended functionality**
  - Trusted Service Engine (TSE)
  - Cross-domain database access
  - Other web services

Summary: Trusted Service Engine