IS&GS DEFENSE

A Systems Engineering Approach to Multi-Level Security in a Service Oriented Architecture

Tim Greer
Principal Systems Engineer
301-788-4882

LOCKHEED MARTIN

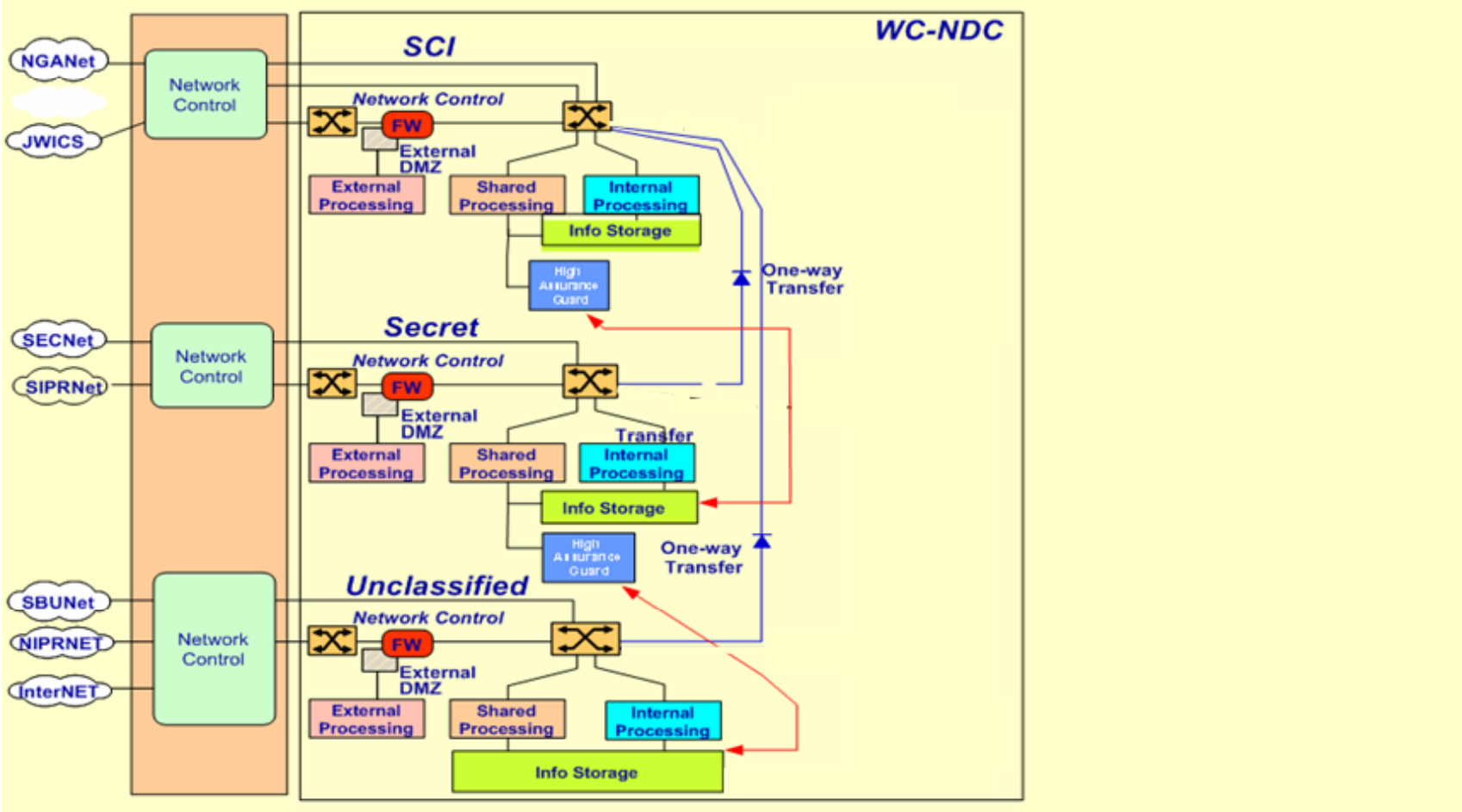
Presentation Overview

- Definitions
- Architecture Approach
  - Requirements Analysis
  - Security Layers – OEM Layers
  - Threats and Countermeasures
- Design Considerations
- Performance Considerations
- Cost Considerations
- Conclusion

Definitions

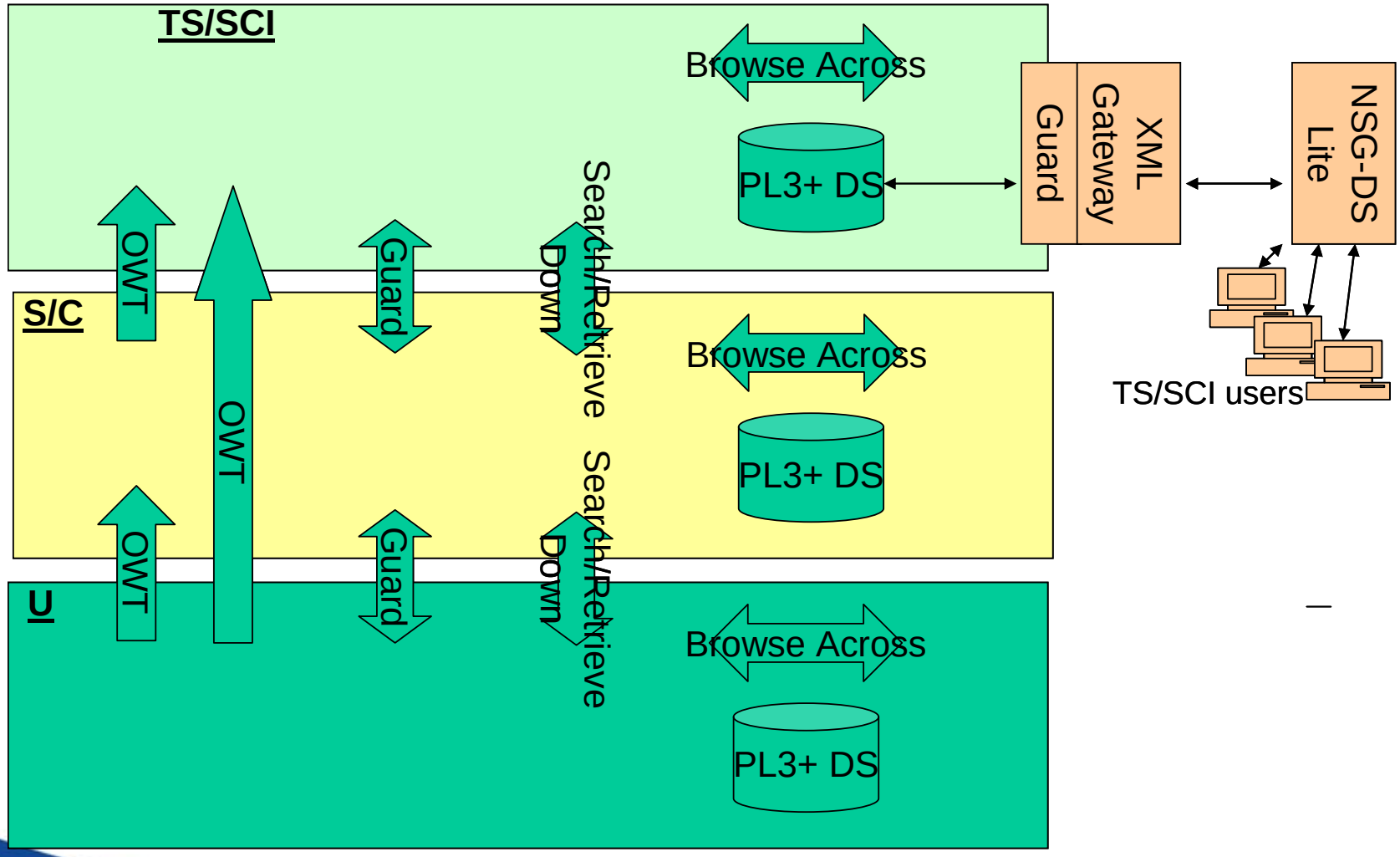
- Multi-Level Security (MLS) VS Multiple Security Levels (MSL)
  - MLS – Data from different security classification levels on the screen at the same time or
  - MLS – Data from different security classification levels or releasability restrictions stored in the same data base
  - MSL – Multiple security enclaves co-located but physically separated
  - MSL – Data from only one security enclave on a screen at a time – KVM switch may connect to workstation to multiple security enclaves – but each must be logged into separately

Multiple Security Levels (MSL)

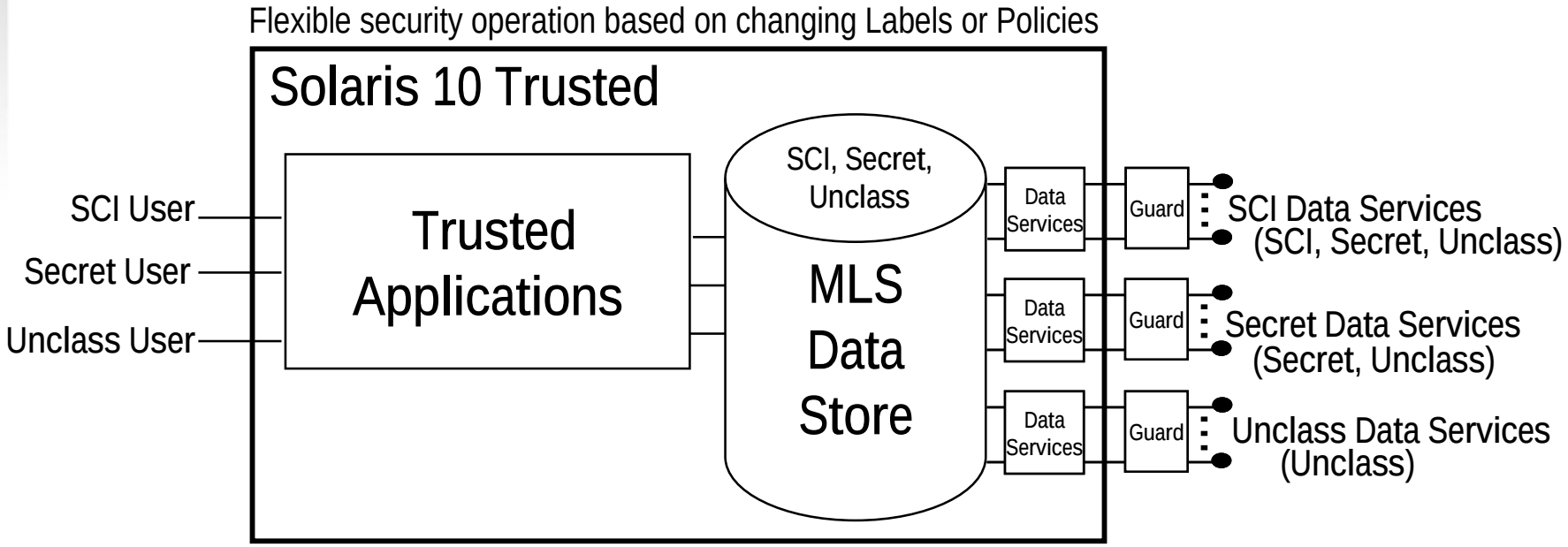


IS&GS DEFENSE

Multi-Level Security - Definition 2



Multi-Level Security – Definition 1



Definitions

- Service Oriented Architecture
  - A standards-based architectural paradigm that enables mission processes through discovery and invocation of published, shared, discrete, and reusable mission and infrastructure services across a network
  - Designed to allow a community of service providers and consumers to achieve value by aligning services to mission processes and enabling better mission agility
  - Services are published, discoverable, invoked, and consumed
  - Services may be discovered and consumed either internally or externally to an enterprise
  - Services are designed to be predominantly loosely coupled however a family of services may be built and designed to work together

Definitions

- Authentication - Establishes, verifies, and identifies a person or a process – includes identity assertion.
- Authorization - The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.
- Role Based Access Control (RBAC) – The process of restricting access to a service resource based on the roles associated with the consumer log in.

Requirements Analysis

- The following information must be collected prior to contacting the Designated Accreditation Authority (DAA)
  - The category, classification, and all applicable security markings for all of the information on, or to be put on, the system;
  - The need-to-know status of the users on the system, including their formal access approval(s), clearance(s), and nationality(ies);
  - The perimeter and boundary of the system;
  - The operating environment of the system and connecting systems, including the service provided (e.g., electronic mail, Internet access), and foreign access to the system, connecting systems, and the facilities housing these systems; and
  - The technical and administrative security requirements of the system.

Architecture – Requirements Analysis

- Security Requirements are often not explicitly stated
  - Look for:
    - Data transfer requirements
    - Access to a particular network or the internet requirements
    - Visualization of data requirements
    - Reference to a directive or standard requirements
    - Connection to applications or systems (interoperability) requirements
  - When connecting to networks like SIPRnet, JWICS, NGAnet, NSAnet, DIAnet, NIPRnet, CENTRIX
    - Contact the Designated Accreditation Authority (DAA)
    - Obtain the appropriate STIGS, SNAC Guides, DCID 6/3, MAC

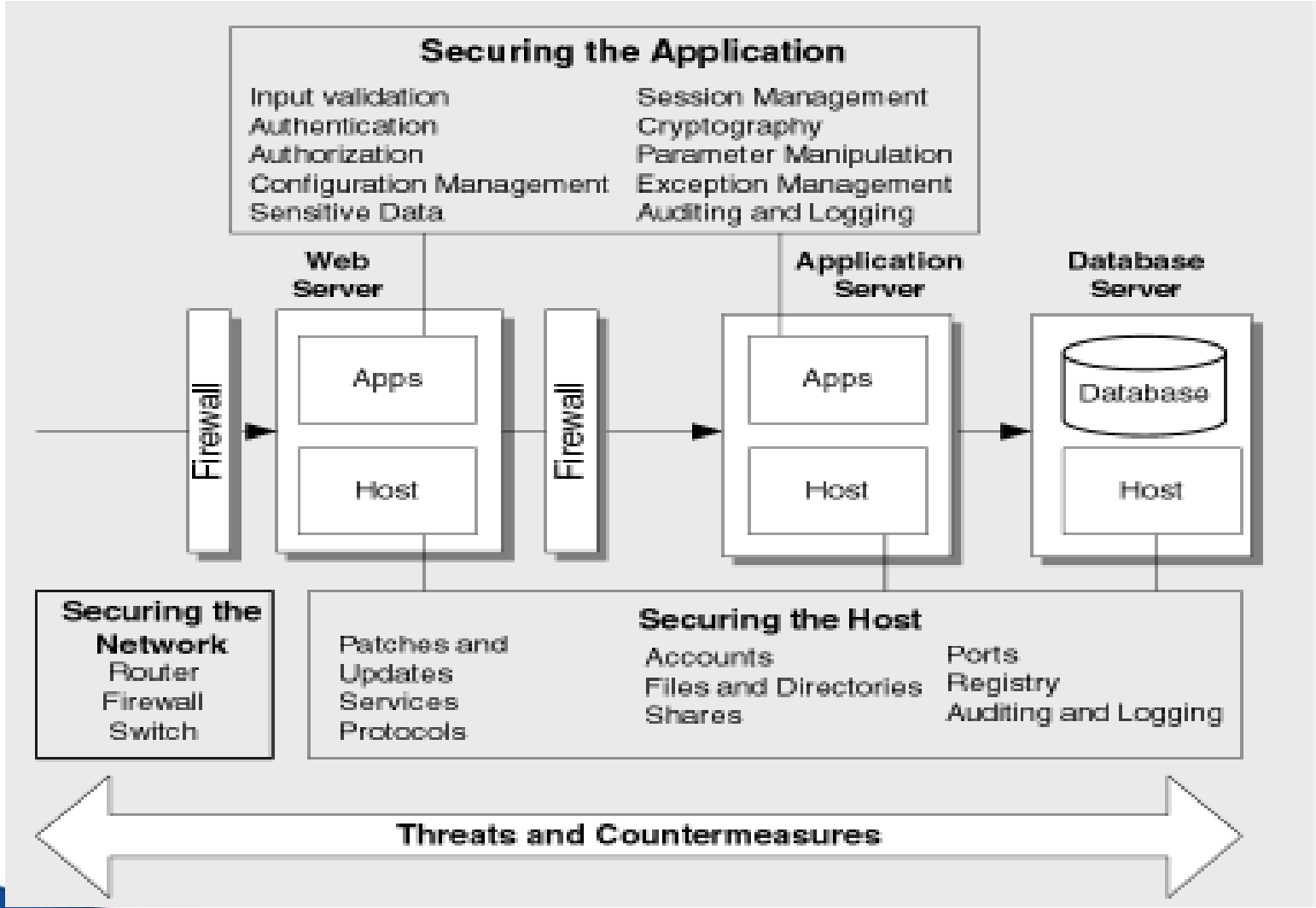
Dissemination Requirements

- **DCID 8 States:**
  - **Maximize Production of Intelligence at Multiple Security Levels.**
    - **Write-to-Release**
    - **Tearlines**
    - **Content Management**
    - **Data Tagging**
- **ICD 501 States:**
  - **IC elements shall have a predominant responsibility to:**
    - **Provide**
    - **Discover**
    - **Request relevant information**

Requirements Analysis

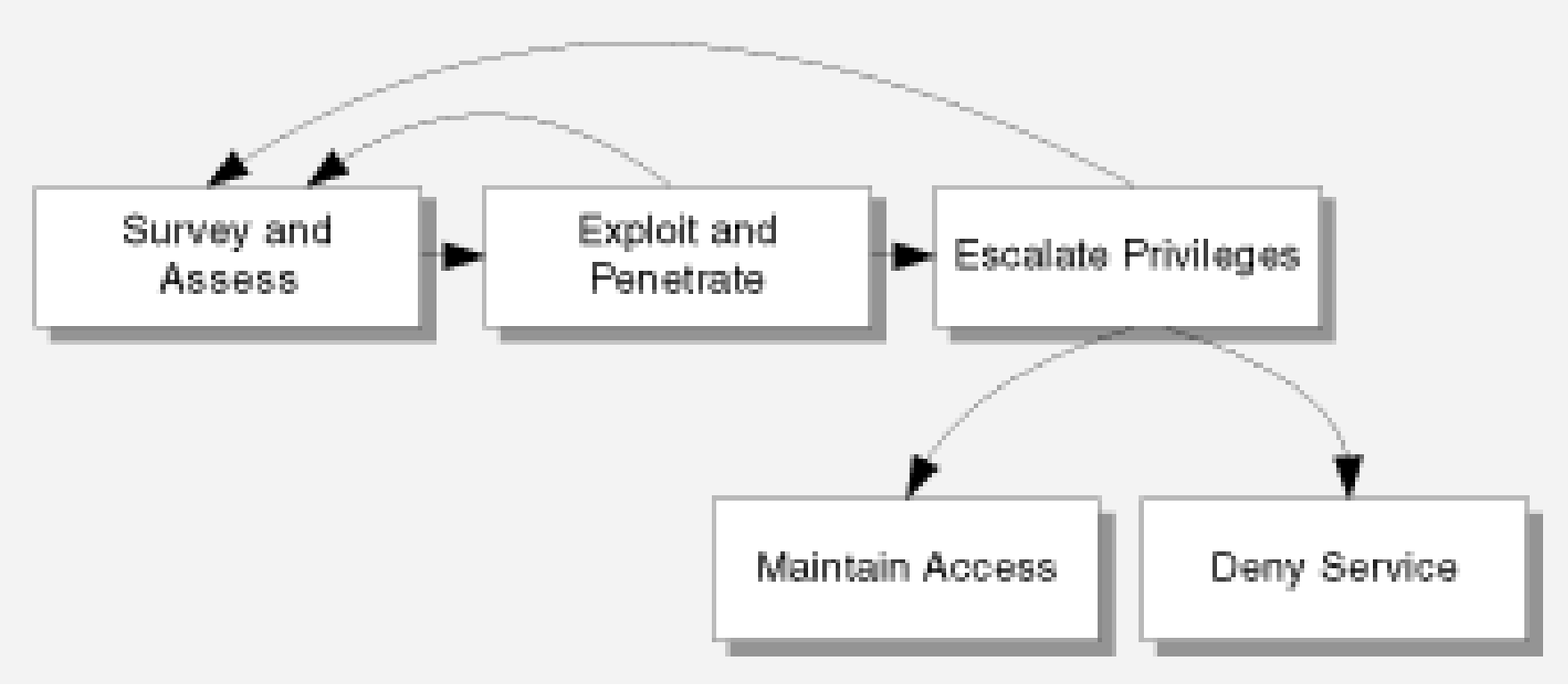
- DIACAP Training – http://iase.disa.mil/eta/diacap/diacap1/index.htm
- DCID and ICD guides http://www.fas.org/irp/offdocs/dcid.htm
- DCID 6/3 Online Manual http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm
- *Intelligence Community Directive Number 501 www.dni.gov/electronic_reading_room/**ICD_501**.pdf*
- DoD Metadata Specification https://metadata.dod.mil/mdr/irs/DDMS/

Threats & Countermeasures



IS&GS DEFENSE

Anatomy of a Threat



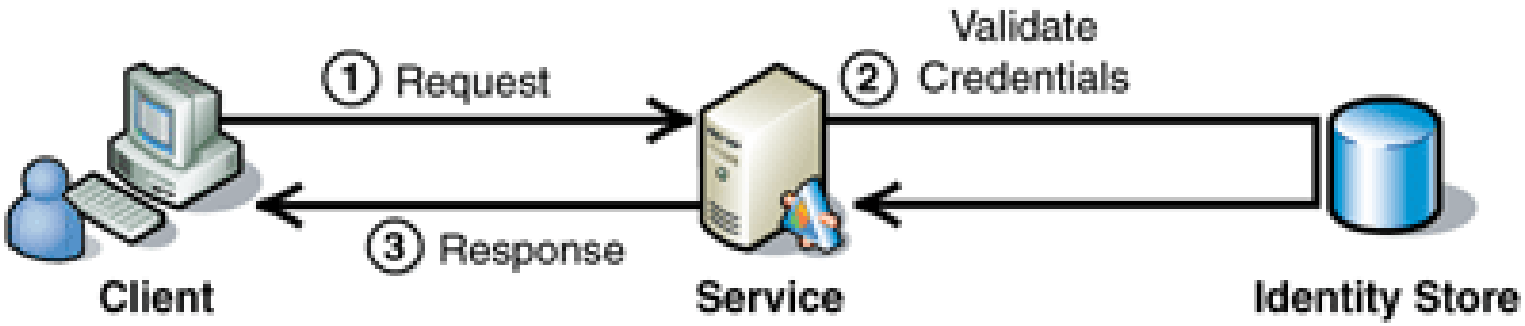
Threats

- **Spoofing**
- **Tampering**
- **Repudiation**
- **Information disclosure - Sniffing**
- **Denial of service**
- **Elevation of privileges**
- **Session Hijacking**

Countermeasures

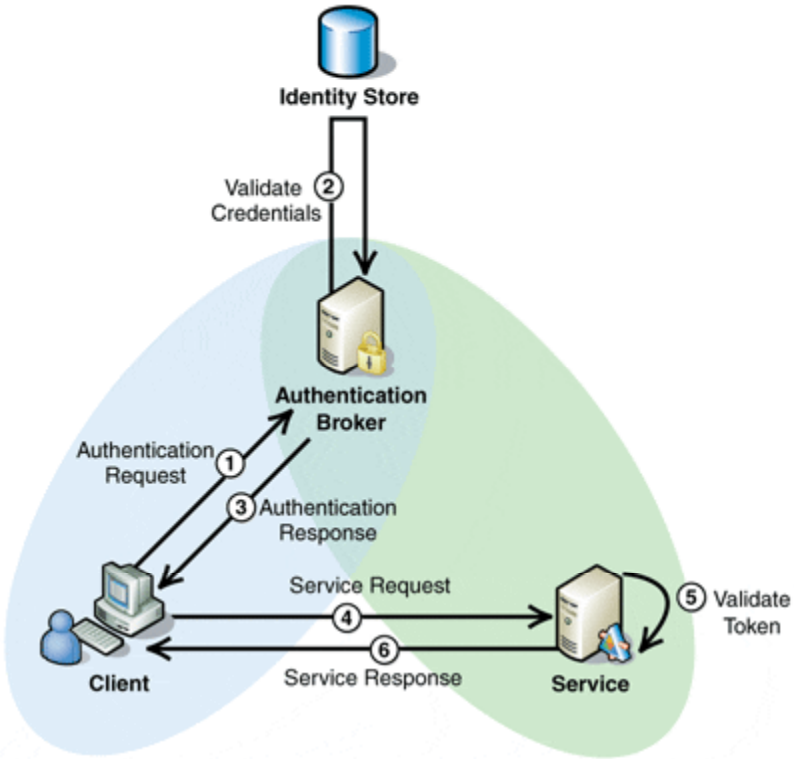
- Spoofing **– Strong Authentication (Cetificates) – Mutual Authentication – SSL - Encryption**
- Tampering **– Strong Authorization – Data Hashing – Digital Signatures – Message Validation Protocols**
- Repudiation **– Secure Audit Logs – Digital Signatures**
- Information disclosure – Sniffing – **Strong Encryption - SSL**
- Denial of service – **Intrusion Detection System (IDS) – Defense in Depth – Buffering and Resource Throttling Techniques – Validate & Filter Input**
- Elevation of privilege **– XML Gateway – Use Least Privileged User Accounts**
- Session Hijacking – **Strong Encryption – Timestamp Synchronization & Re-authentication**

Design Considerations – Direct Authentication



Design Considerations – Brokered Authentication – Mutual Authentication

- Kerberos Ticket
- X.509 PKI Certifi
- STS

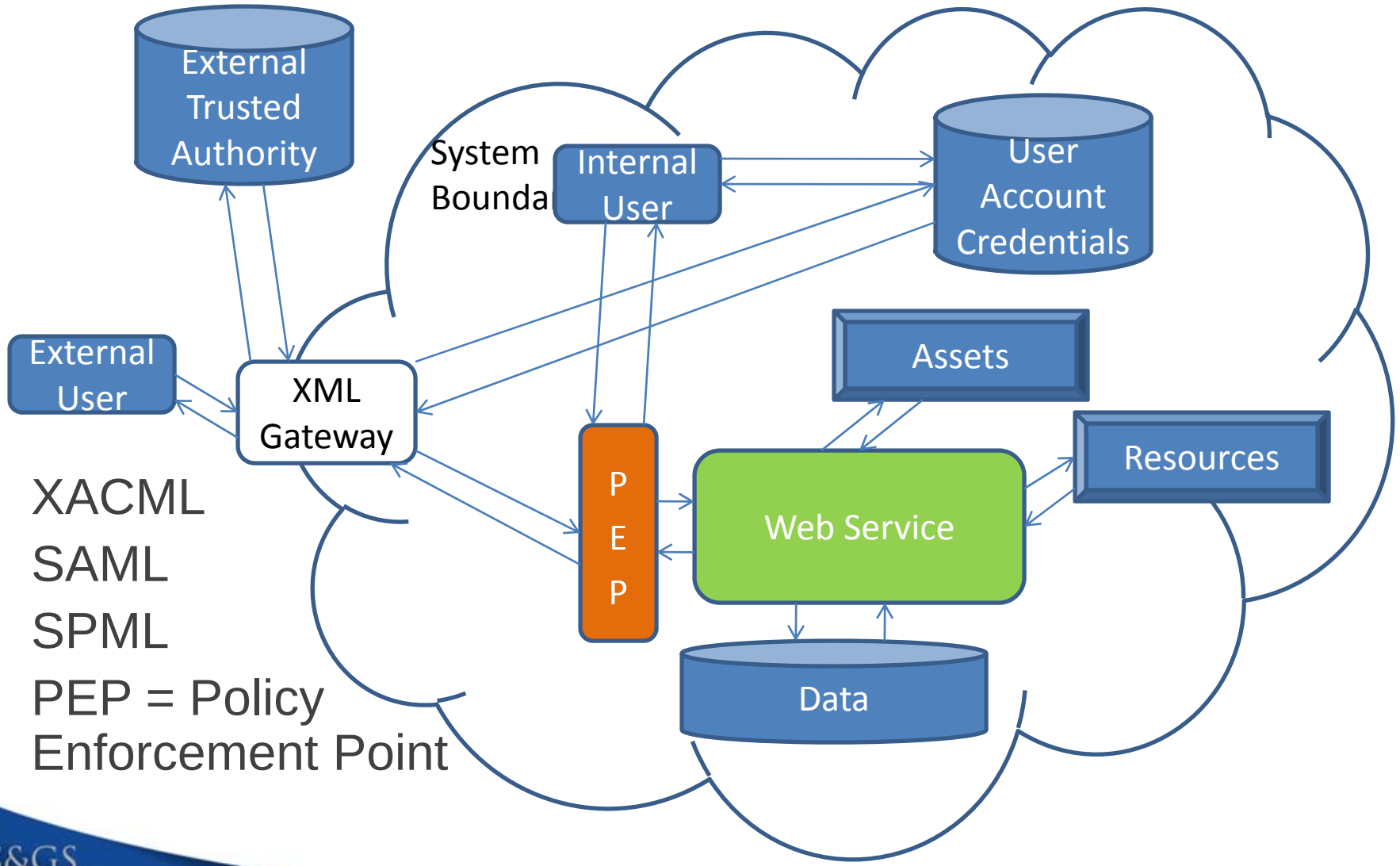


IS&GS DEFENSE

Message Layer VS Transport Layer Security

- Brokered Authentication can be implemented at the Message Layer or Transport Layer
  - Message Layer Security provides for
    - Data Confidentiality
    - Data Origin Authentication
    - Data Integrity
  - Message Layer Security is more complex
  - Transport Layer Security provides for
    - Minimal code and configuration work
    - With Kerberos can work across multiple system hops
  - Transport Layer is simpler – but does not provide Data Integrity – should be used with SSL
    - SSL can only be used point to point VS end to end

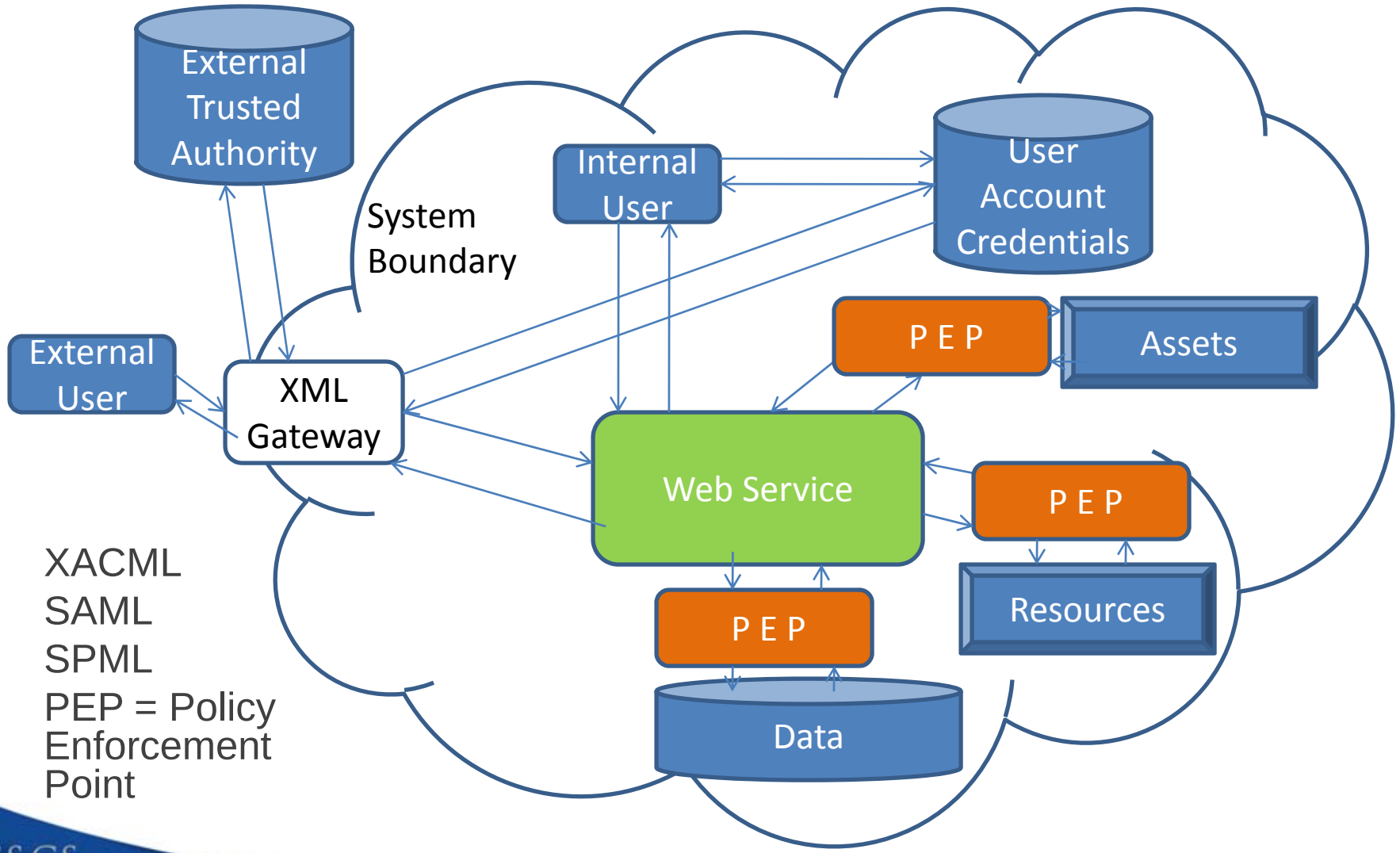
Policy Enforcement



- XACML
- SAML
- SPML
- PEP = Policy Enforcement Point

IS&GS DEFENSE

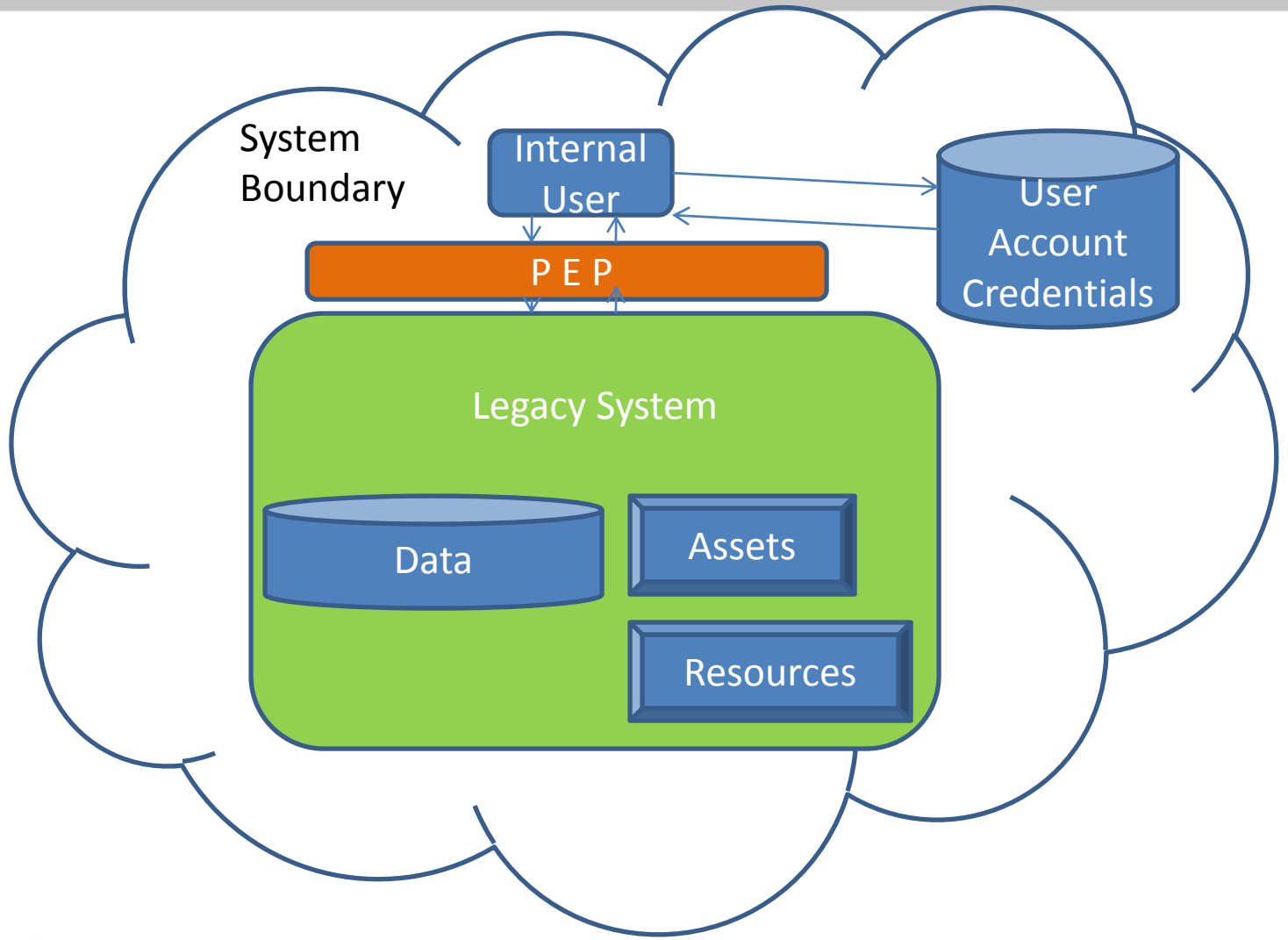
Policy Enforcement



- XACML
- SAML
- SPML
- PEP = Policy Enforcement Point

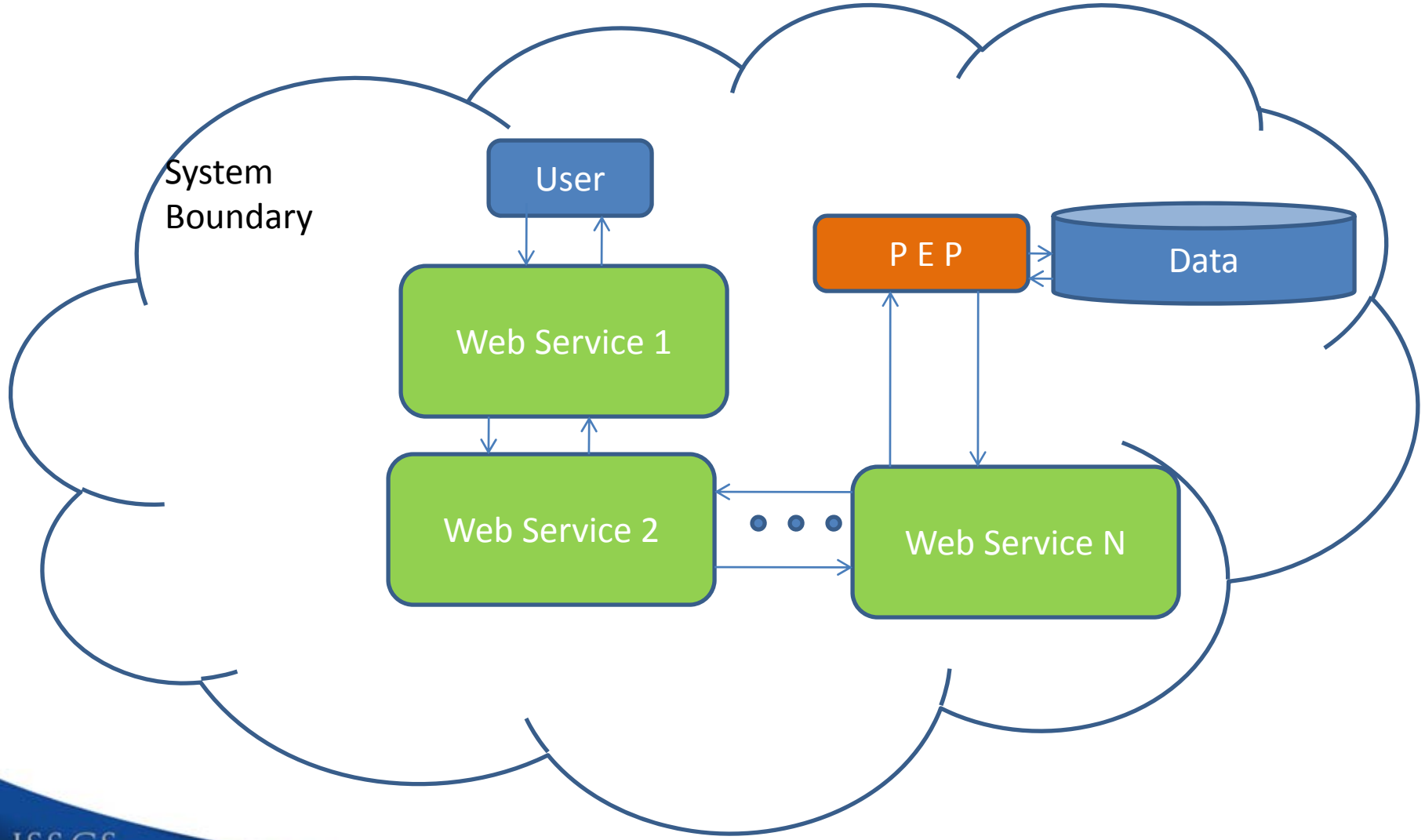
IS&GS DEFENSE

Policy Enforcement



IS&GS DEFENSE

Trusted Subsystem



Logging and Auditing

- **Ensure all audit records include date and time of action, the system locale of the action, the system entity that initiated or completed the action, the resources involved, the action involved, and successful and unsuccessful logons and logoffs.**
- **Protect the contents of audit trails against unauthorized access, modification, or deletion.**
- **Maintain collected audit data at least 5 years and review at least weekly.**
- **Maintain an audit trail that includes selected records of: Accesses to *security-relevant* objects and directories, including opens, closes, modifications, and deletions.**
- **Maintain an audit trail that includes activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users.**
  - **Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual).**
  - **Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools.**

Cost and Performance

Criteria	Definition	Rank	Weight
Standard Evaluation Criteria			
Cost	Includes both the recurring and non-recurring costs. Include labor, resources and any lifecycle charges.	5 – Very Low Cost Impact 4 – Low Cost Impact 3 – Medium Cost Impact 2 – High Cost Impact 1 – Very High Cost Impact	15%
Meets Requirements	Indicates the ability of a solution to fully and or partially meet the requirements defined in the A-specification and B-Specification	1 – Very Low Meets Requirements 2 – Low Meets Requirements 3 – Medium Meets Requirements 4 – High Meets Requirements 5 – Very High Meets Requirements	20%
Install Base	Defines how widely used a solution is and how many users may be trained on the solution today. Not specifically meant to portray commercial use, it also includes GOTS standards that have been adopted by gov't agencies.	1 – Very Low Install Base 2 – Low Install Base 3 – Medium Install Base 4 – High Install Base 5 – Very High Install Base	5%
Performance	Indicates the speed and quality at which a solution executes its functions. If possible, it should be based on hard execution data. If this is not feasible, the measure can be based on the architectural choice made that may enhance or impede performance. It also considers the consistency of the performance for all the users	1 – Very Low Performance 2 – Low Performance 3 – Medium Performance 4 – High Performance 5 – Very High Performance	10%

IS&GS DEFENSE

Cost and Performance

Criteria	Definition		Rank	Weight
Standard Evaluation Criteria				
Dependencies	Defines the number of strict needs the solution requires to operate. These dependencies can be at the infrastructure level or at the system level. Should be an indicator of how easy it will be to integrate the solution.	5 – Very Low Dependencies 4 – Low Dependencies 3 – Medium Dependencies 2 – High Dependencies 1 – Very High Dependencies	5%	
Certification & Accreditation	Indicates if the solution has been accredited previously. If not, it should provide some measure that indicates if it would be easily accredited based on similar products, its lifecycle, its implementation etc…	1 – Very Low Certification & Accreditation 2 – Low Certification & Accreditation 3 – Medium Certification & Accreditation 4 – High Certification & Accreditation 5 – Very High Certification & Accreditation	5%	
Interoperability	Defines the solution's capability to interoperate with diverse systems and infrastructure capabilities. Indicates if the solution is based on open (non-proprietary) standards, that it has exposed interfaces and is adaptable to many environments. This also includes the product's ability to operate in service oriented environment.	1 – Very Low Interoperability 2 – Low Interoperability 3 – Medium Interoperability 4 – High Interoperability 5 – Very High Interoperability	5%	
Reliability	Measures a solution's ability of a system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances. Systems with no track record or with complex, unreliable software will probably score lower.	1 – Very Low Reliability 2 – Low Reliability 3 – Medium Reliability 4 – High Reliability 5 – Very High Reliability	5%	

Cost and Performance

Criteria	Definition	Rank	Weight
Standard Evaluation Criteria			
Manageability	Requires the product to be capable of being managed in a production	1 – Very Low Manageability 2 – Low Manageability 3 – Medium Manageability 4 – High Manageability 5 – Very High Manageability	5%
Scalability	Defines a products capability to add additional hardware or software to the system for additional load (i.e. additional users, messages, clustering).	1 – Very Low Scalability 2 – Low Scalability 3 – Medium Scalability 4 – High Scalability 5 – Very High Scalability	5%
SWAP Impact	Defines the impact on the existing deployed system for space, weight and power availability.	5 – Very Low Hardware Impact 4 – Low Hardware Impact 3 – Medium Hardware Impact 2 – High Hardware Impact 1 – Very High Hardware Impact	15%
Flexibility	Defines the additional capabilities the product adds to the trade over and above the basic requirements for solutions to other complexities of the system (i.e. real time changing of logging levels, monitoring of metrics, debugging of service transactions, configurable)	1 – Very Low Intelligence Community Standard 2 – Low Intelligence Community Standard 3 – Medium Intelligence Community Standard 4 – High Intelligence Community Standard 5 – Very High Intelligence Community Standard	2.5%
Intelligence Community Standard	Defines the compliance with DCID 6/3.	1 – Very Low Intelligence Community Standard 2 – Low Intelligence Community Standard 3 – Medium Intelligence Community Standard 4 – High Intelligence Community Standard 5 – Very High Intelligence Community Standard	2.5%

Gartner's Magic Quadrant

Ability to Execute

(In Technology, visibility, services, features)

Focus on Tomorrow →

Challengers	Leaders
Execute well today or may dominate a large segment, but does not yet understand market direction	Executes well today and is well-positioned for tomorrow
Focuses successfully on a small segment, or is unfocused and does not out innovate or outperform others	Understands where the market is going or has a vision for changing market rules, but does not yet execute well
Niche Players	Visionaries

↑

Accreditability

- Evaluation by independent Laboratories – Common Criteria http://www.commoncriteriaportal.org/
- Early Engagement of DAA
- Thorough testing using the STIGS, SNAC Guides and other guiding documents
- Well documented architecture
- Well documented system and operational procedures

Conclusion

- Engage DAA Early
- Requirements Analysis early and complete
- Identify Threats
- Determine Countermeasures
- Evaluate Architecture Alternatives
- Balance Cost, Performance, Security through Analysis of Alternatives exercise
- Leverage Existing Capabilities While Implementing New Technologies

IS&GS DEFENSE

A Systems Engineering Approach to Multi-Level Security in a Service Oriented Architecture

Tim Greer
Principal Systems Engineer
301-788-4882

QUESTIONS

LOCKHEED MARTIN