Net Centric Enterprise Services Information Assurance Challenges and Recommendations

5 March 2004

Security Issues –Net Centric Services

- Information Assurance Subcommittee

– Glenda Turner	OSD/DOD
– Kevin T. Smith	McDonald Bradley
– Chuck Olsick	McDonald Bradley
– John Warther	Green Hills Software
– Tom Mayhew	Oracle
– Courtney Edwards	Boeing
– Mike Smeltzer	Northrop Grumman
– Joe Bergmann	The Open Group
– Greg Wenzel	Booz Allen
– Arnie Rausch	Eagan McAllister
– Frank Graves	Mitre Corp

Security Issues –Net Centric Services

Policy Issues

Definition – Information Assurance

DoD 8500.1:

“Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.”

Policy Issues - 1

- Management of Emerging Threats
  - A robust IA program managed by DOD and coordinated with the NSA (Information Assurance Technology Framework Forum), STRATCOM, DISA, JFCOM, and others
  - Aggressive enforcement of CERT Bulletins
- Management of Authorization Credentials
  - Identity Management is a challenge, but Issues with Need To Know/Security Roles Across Different Networks are more challenging.
    - Who will manage authorization credentials?
  - Suggest Establishment of Enterprise-Wide Security Roles Shared by All Participants and Partners
    - Let these roles have security policy associated with them, and let data producers manage their own roles, if not addressed by enterprise roles.
    - Allow access control to the data sources be protected by the providers themselves (using these roles)

Policy Issues - 2

- DCID 6/3 Protection Level Issues:
  - Policy on repositories of clearance information for users in network federation?
    - In order to achieve a higher protection level, trusted applications will need to go to an authority explaining need-to-know for a user
    - Suggest a standards-based authorization server that will provide these access control decisions for our trusted applications.
  - Horizontal Fusion ultimately has a PL/5 Goal, but needs to address these policy issues
- Tagging and Policy on Trusted Authorities
  - Data needs to be tagged with an appropriate classification level and digitally signed
  - Digitally signed data tagged with classification levels meets non-repudiation of security label; who is the trusted authority that does the labeling and signing?
    - The technical part is not the challenge – understand <u>who to trust</u> (a policy decision) is.
  - Digital Signatures need to be in every part of the process – from production and query..

Policy Issues - 3

- Trust of COTS?
  - Confidence level dependent upon access to the COTS source code
    - CONUS developed code could undergo C&A and would require certification by the vendor that the code was developed solely by U.S. citizens
    - OCONUS developed COTS source code and any upgrades thereafter could undergo IV&V and C&A before “approved for net-centric use”
  - OCONUS developed code could be prohibited from use
  - Assign responsibility to coordinate or centralize DOD and Intel related COTS software assurance testing and validation initiatives
    - Joint Interoperability Test Command
    - DISA center
    - NIST (Common Criteria Test Labs)
    - NIAP Certification for COTS

Security Issues –Net Centric Services

Requirements Issues

Requirements Issues

- Security Scope- What are the “Rules” for security in a “pull” environment?
  - Roles, responsibilities, and security levels can be defined for the “user level”, but centralized governance and “control” must be determined
    - Guard technologies show promise
    - Message Filtering Technologies (in Engineering Slide) also shows promise
- Evaluation – How do you evaluate Net-Centric Services for security and where is the end of the evaluation?
  - A Defense in Depth strategy to protect the network infrastructure, enclave boundaries, and the computing environment as well as protecting PKI/KMI and the ability to detect and respond is needed. Consider:
    - Authenticated access control
    - Data integrity
    - Redundant paths
    - Hardened systems
    - Strong encryption
    - Traffic flow security measures
    - Boundary devices for access control, filtering, etc
    - Distributive intrusion detection
    - Security enabled applications
    - PKI
    - Backup and restoration, alternate paths
    - Physical security and other measures
    - **Network-based Covert Channels?**
  - Establish formal methods for software OS, Middleware, applications, and network protocol evaluation
  - Formal and rigorous processes for C&A and managing systems and data

Security Issues –Net Centric Services

Engineering Issues

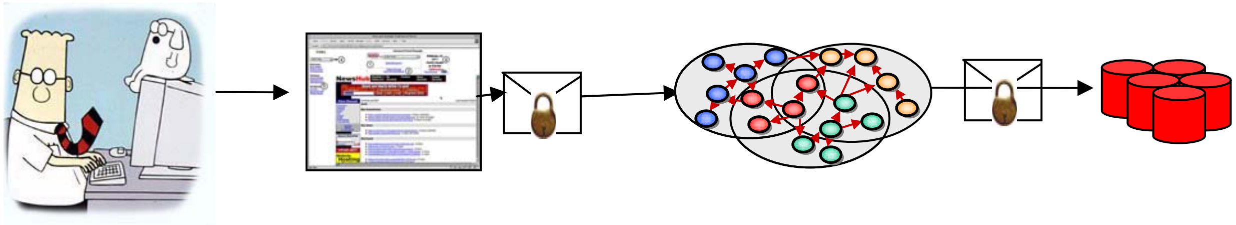
Engineering Issues – 1

1. Open Standards vs. Proprietary or Non-Standard APIs
    - If the DoD tries to dictate certain security APIs for everyone to use, we will move from "Net Centric" to "Implementation Centric".
    - We need to dictate Specifications based on Open Standards – (wire formats, not implementation)
        - WS-Security SOAP Messaging
        - XML Signature
        - SAML (Security Assertion Markup Language)
    - Keep an eye on the standards bodies and commercial vendors to see what is truly supported
        - Ex: XACML vs. WS-Policy?
        - Ex: Project Liberty vs. WS-Federation?
        - Will All of WS-Security Specs be Adopted?

Engineering Issues –2

2. Encryption – Capability at Data Layer <u>and</u> Packet Layer

- Encryption at “Packet Layer”
  - Sometimes bulk encryption (IPSec/SSL between nodes) is a requirement for confidentiality of traffic
- Encryption at “Data Layer”
  - Sometimes bulk encryption does not solve the requirements – using a standard such as XML Encryption could be used for encrypting <u>only the</u> confidential data between the user and the data source

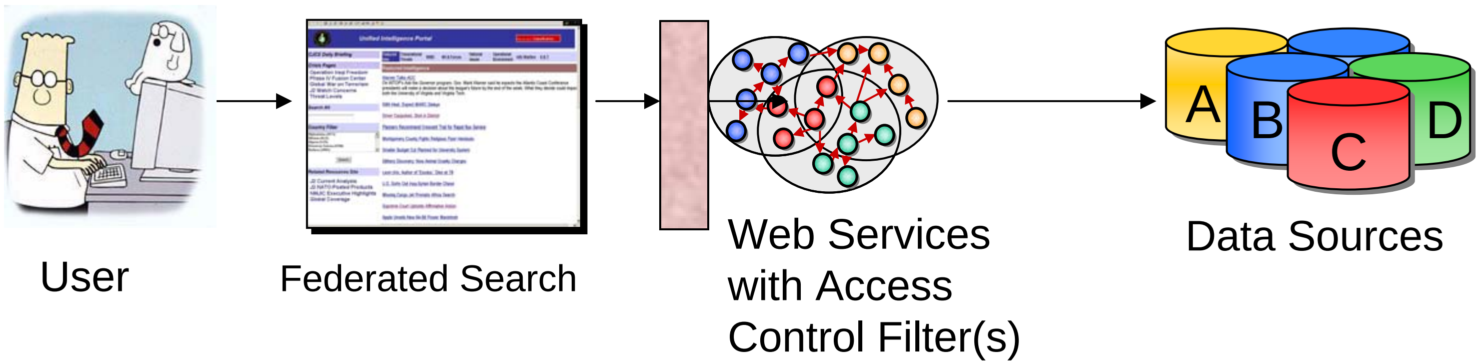


Engineering Issues – 3

3. Identity and Authorization Management
   - Of users themselves – X.509 Certs bind identity to public keys
   - Of their credentials – what they are allowed to do, security roles, clearances
     - Technically feasible, but who manages these credentials?
   - Relates to Policy – Enterprise Roles for RBAC
     - Who will manage access control policy stores in NCES?
     - Need the flexibility of data sources managing policy – as well as enterprise-wide access control policy
   - Suggest an authorization server (that maps authorization credentials to network identities) managed centrally, but providing the opportunity for data sources to be able to <u>extend</u> this for data source-specific rules

Engineering Issues – 4

4. Federated Search aggregating content from multiple data stores
   - Need to filter based on user’s security role, classification level
   - This can be technically accomplished at the SOAP Filter Level – but what about classification of dynamic content creating new classification?



User

Federated Search

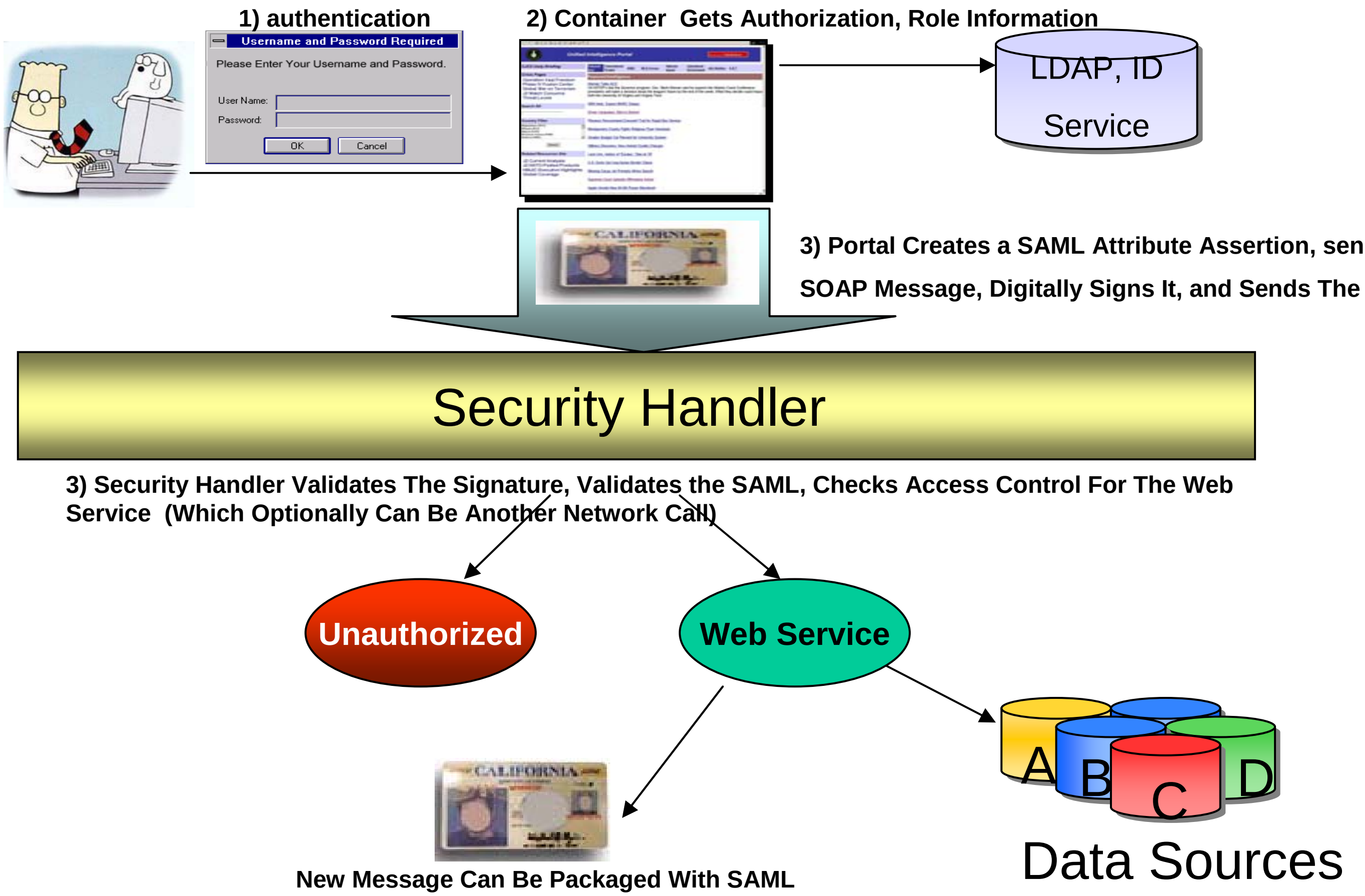
Web Services with Access Control Filter(s)

Data Sources

Engineering Issues - 5

5. Trust Propagation/Single Sign-On with Web Services
   - Need Federated Identity Solution; Since Web Services can be chained together to orchestrate solutions, we need to be able to pass the end-user’s identity from point to point to point
   - This also affects Single Sign-On when data sources expect authentication credentials other than the centralized service

Engineering Issues –5 (cont.)
Trust Propagation Solution



1) authentication

2) Container Gets Authorization, Role Information

3) Portal Creates a SAML Attribute Assertion, sends it with SOAP Message, Digitally Signs It, and Sends The Message

3) Security Handler Validates The Signature, Validates the SAML, Checks Access Control For The Web Service (Which Optionally Can Be Another Network Call)

New Message Can Be Packaged With SAML

Engineering Issues - 6

- Secure Directories and Data Authority/Modification – How do we prevent unauthorized changes during discovery?
  - Mutual authentication with SSL connecting with directories, UDDI services
  - Only Trusted agents should be able to get identity/authorization information

- Defensive Information Warfare
  - Need to proactively protect from attack..
    - IP/Server Spoofing
    - Message Injection
    - Message Replay attacks
    - Denial of Service
  - ➢ We will need to focus on Intrusion Detection based on Signatures of Known Attacks, as well as "smart" IDS functionality for anomaly detection

Engineering Issues - 7

- Need Agile and Flexible Security Solutions
  - Although we are “network centric”, realize that there can be security performance issues with each network call:
    - If we provide a web service for every security function, realize that:
      - You will need to cryptographically protect each network call
      - The response of each web service message should be digitally signed (and then validated by the caller)
      - There may be network latency issues
      - If the network goes down – or if web service is attacked, where does the security go??
  - “Centralized” vs. “Decentralized” – not one of these answers is correct.
    - Suggest a flexible architecture that has security components at each provider, and network-based services.
      - Each component has the capabilities of security web services (signature validation, policy decision service) – but can do them locally
    - Such a solution promotes agility and countermeasures to network attack

Next Steps

- Coordinate, Coordinate, Coordinate
  - Set the IA Standards
  - Define a Flexible IA Architecture
  - Set the Policy on a Coordinated Basis