IBM Federal

Security Working Group Kickoff

David White
John McLaughlin
Norman Sadeh

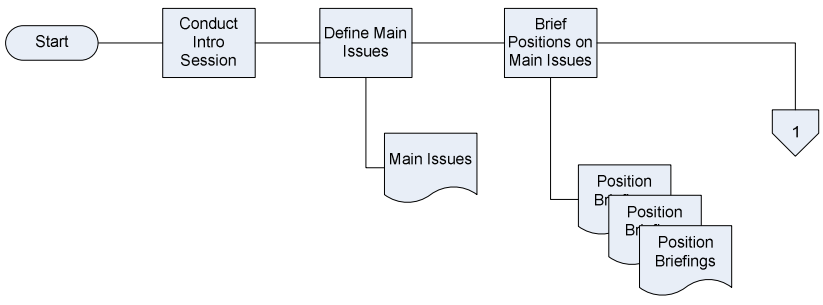
Objectives

- **Our Objective**
- **Our Problems**
- **Specific Problems**
- **IBM Security Reference Architecture**

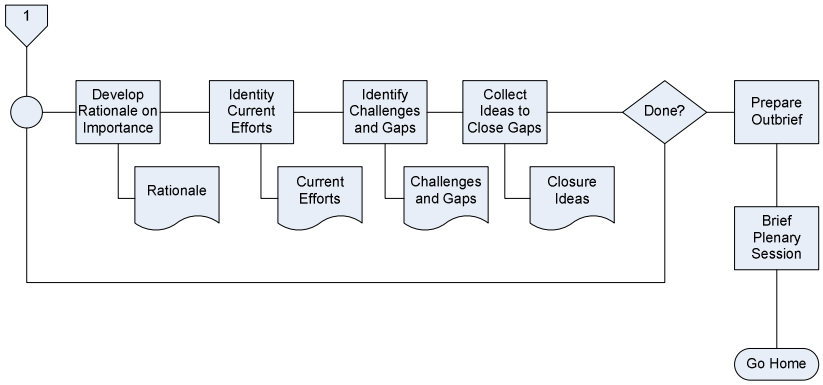
The Schedule

- 10:15 – 12:00 Morning working sessions
  - 10:15 – 10:45 Orientation; brief position statements
  - 10:45 – 11:00 Focus on 2 or 3 topics
  - 11:00 – 12:00 Discussion of selected topics (template to be provided)
- 12:00 pm Working Lunch (provided free of charge)
- 1:00 pm – 230 Continuation of Working Sessions and Brief Out
  - 1:00 – 2:00 Continuation of discussion
  - 2:00 – 2:30 – preparation of brief out reports

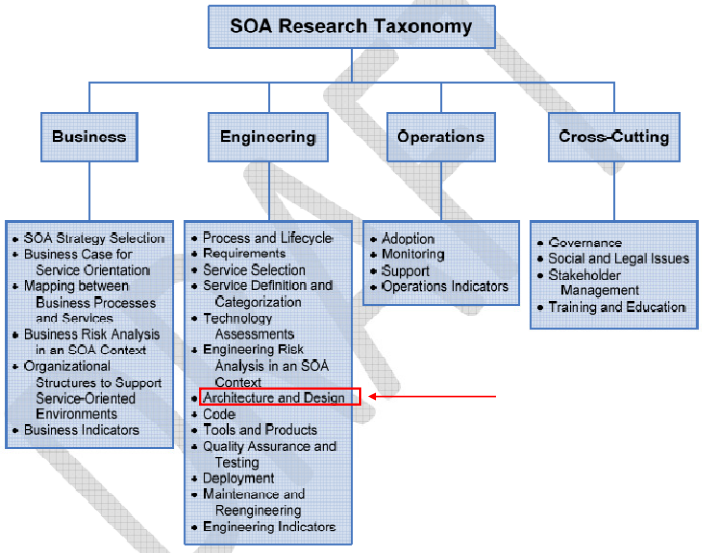
Today's Workflow (1 of 2)



Today's Workflow (2 of 2)

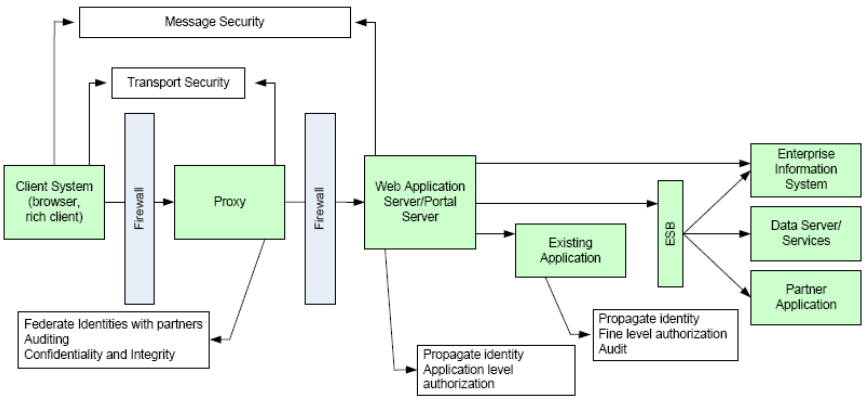


Constraint: Must Map to SOA Research Taxonomy



Development of Main Issues

Typical Logical Deployment Architecture



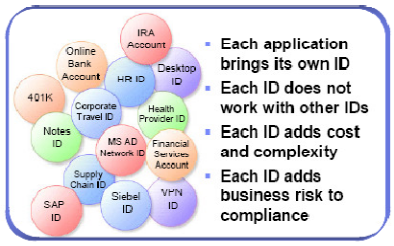
Two Key Strategic Challenges are Observed

- Security infrastructure integration challenge
  - Multiple identity and authentication systems, multiple authorization engines and multiple audit points are typically not well integrated
- Security mediation challenge
  - Multiple islands of product-specific administration
  - Prone to error and inconsistency
  - Management often business unit specific
  - Required to be enterprise wide

Five Main Issues from the Key Challenges

- **User Identity**
- **Real Time Transaction Integrity**
- **Composite Application Complications**
- **Managing Security Across Diverse Applications**
- **Protecting Data**

SOA Security Challenge -User and Service Identity Challenges



- **Greater number of diverse users**
  - Each application/service brings its own IDs and credentials
  - Need to decouple identities from the applications
- **Business flexibility demands**
  - Multiple, heterogeneous endpoints
  - No more application logic coding – expensive to maintain and support
- **Compliance concerns**
  - Maintain clean user directories in mainframe and lines of businesses
  - Flow auditable application identities from point-of-entry to resources

SOA Security Challenge - Real Time Transactional Connection

- **Inter-organization interaction**
  - Requires that identity and transactional policies be enforced
- **Boundary security services**
  - Services need to provide coarsely grained trust verification
- **Trust relationship**
  - Key management, identity translation, label normalization

SOA Security Challenge - Composite Applications

- A single service has a set of security policies
- Service combination, as in a choreography, will aggregate security policies
- May put policies into conflict
- Policies conflict may overtighten security (bad) or relax policies (really bad)

SOA Security Challenge - Managing Security Across Diverse Environments

- A typical SOA will have many points at which security policy is enforced
- Security enforcement points may use a range of security technologies
- *Swivel chair management is very un-SOA*
- Security policy definition and management required to be consistent across the enterprise
- Consistent policy can then be enforced by the SEP or translated into something they can understand

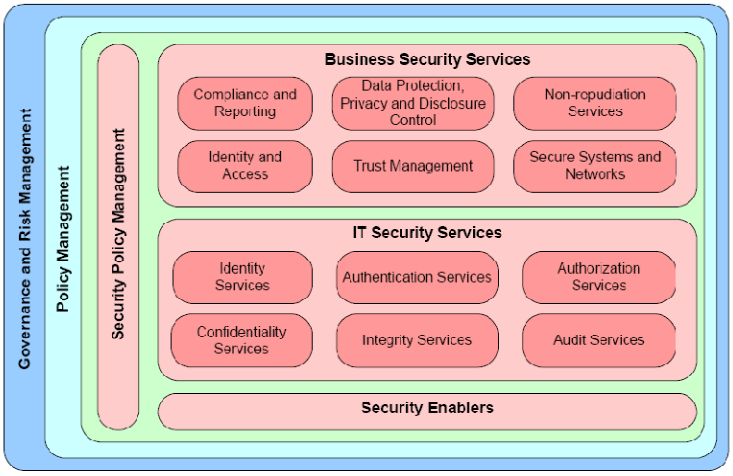
SOA Security Challenge - Protecting Data

- Protection of data from unauthorized modification and disclosure is a key requirement within SOA.
- Consistent security policies critical to protection
- Data may move outside the enterprise with out knowledge of the consumer
- Example is an outsourced service replacing an internal service
- External data security policies are usually different than internal policies

SOA Security Challenge - Regulatory Compliance

- Transaction auditing increasingly required for both external and internal reasons
- Target requirements include internal security policies and external regulatory acts
- Complexity significantly increased when providers and consumers have different levels of compliance
- Audit architecture required
  - Centralized data repository
  - Federated logical views

IBM Security Reference Architecture



Path Forward

- **Assert that these five topics be our domain**
- **Now to select specific topics within these five**
- **Identity what we know**
- **Identify what we don't know**
- **Figure out how to close what we don't know**
- **Prepare out brief to plenary session**