Update on HLA and Security

Philomena M. Zimmerman
ZimmermanPM@navair.navy.mil
(301) 757-4624

Objectives

- Briefing Objective - to provide an update on work underway to support security in the HLA
- Program Objective - formalize the relationship between security and the HLA in a consistent manner, and make it available to both federation users and federation accreditors

Program Background

- Security considerations have been a part of the HLA from the beginning
- TIS initial contractor for security work
- 2 Components to the program
  - Security Certification and Accreditation (C&A) process
  - Runtime Security Architecture investigation

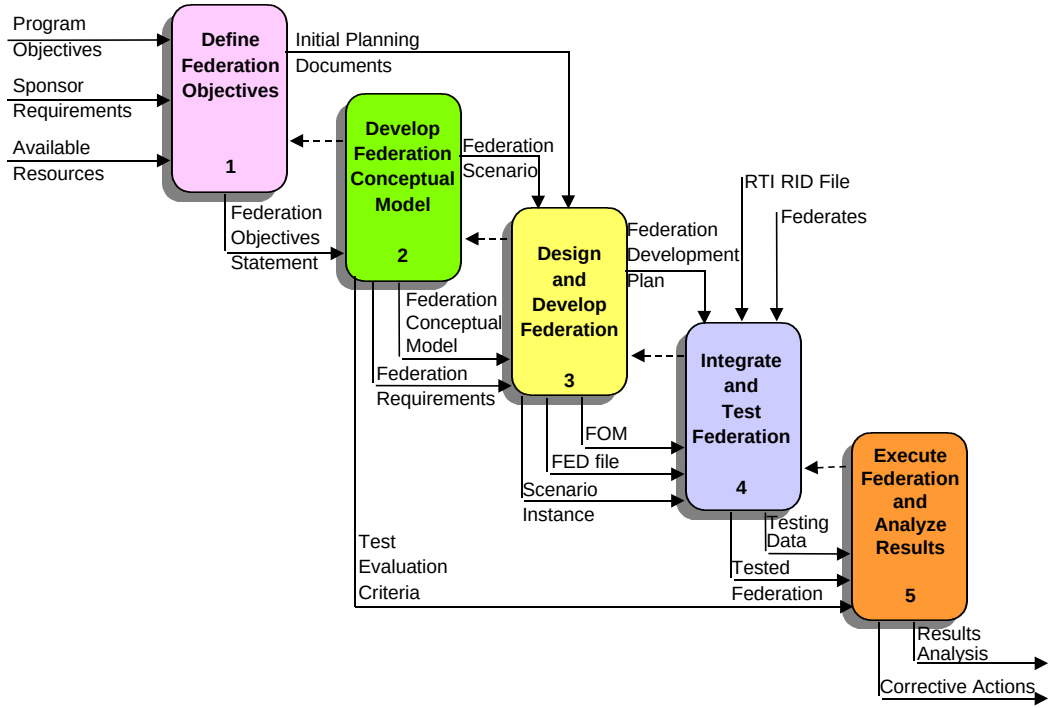
Current Activities

- Supporting Contractor - Corbett Technologies
- Draft C&A process undergoing review
  - Written as a user guide
  - Supplement/overlay to FEDEP
- Feasibility assessment of proposed multi-enclave federation security process delivered in Jan ‘99
  - Includes example SSAA

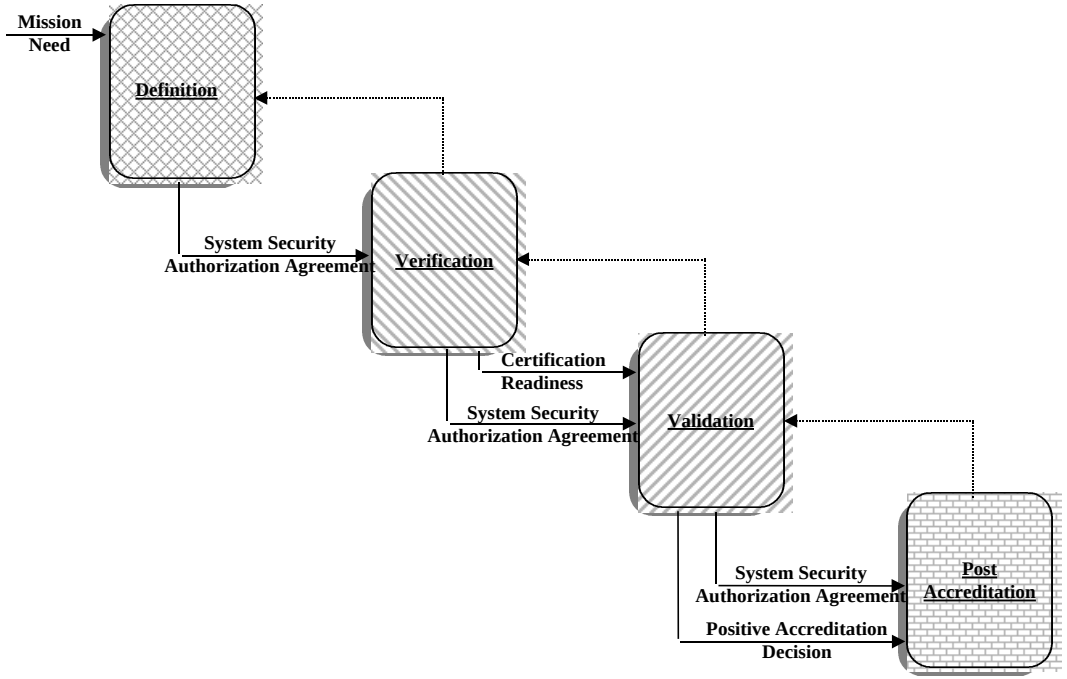
HLA Security C&A Process

- It is based on the entire federation life-cycle
- Through the DoD, there is a general IT security C&A process in place
- This HLA security C&A process maps the general IT security C&A process to the HLA FEDEP
- Past reviews with DISA, Cadre programs indicate we are right on track

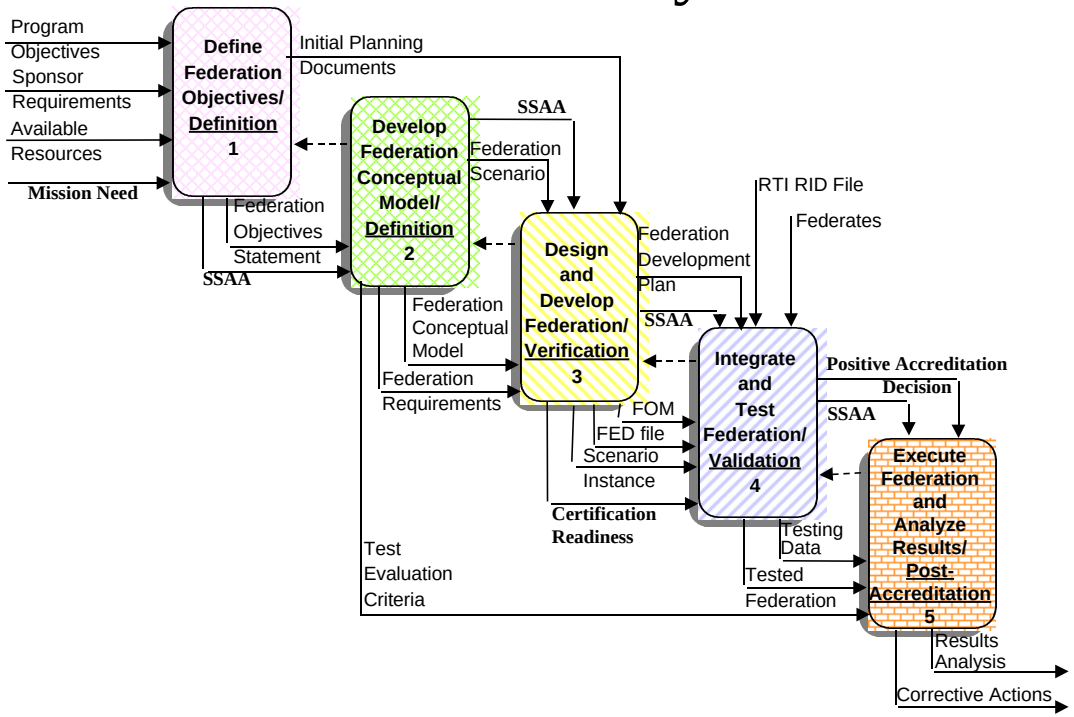
FEDEP


Program Objectives
Sponsor Requirements
Available Resources
Define Federation Objectives
1
Initial Planning Documents
Develop Federation Conceptual Model
2
Federation Scenario
Federation Objectives Statement
Design and Develop Federation
3
Federation Development Plan
RTI RID File
Federates
Federation Conceptual Model
Federation Requirements
Integrate and Test Federation
4
FOM
FED file
Scenario Instance
Execute Federation and Analyze Results
5
Testing Data
Tested Federation
Test Evaluation Criteria
Results Analysis
Corrective Actions

DITSCAP


Mission
Need
Definition
System Security
Authorization Agreement
Verification
Certification
Readiness
System Security
Authorization Agreement
Validation
System Security
Authorization Agreement
Positive Accreditation
Decision
Post
Accreditation

Federation Security Process



FEDEP + DITSCAP = FSP

- Federation Security Policy (FSP) is designed to provide a framework in which to address security throughout the FEDEP process.
- Goal is accreditation and secure use of federation
- Split into 5 phases of FEDEP:
  - Define/Document Objectives + Definition
  - Define Real World Domain + Definition
  - Design Federation + Verification
  - Plan Execution/Integrate Federation + Validation
  - Execute/Analyze Outputs + Post Accreditation

FSP Phase I

- Start by identifying the mission need - to include functions of system, data outputs, possible candidates.
- Identify Program Manager, User Representative, and Responsible security authority
- Identify type of accreditation - for federation execution, or for federation
- Initiate dialog between all parties
  - consistent and open dialogue from this point on is ESSENTIAL to this process
- Begin the SSAA - a “repository” for security documentation

FSP Phase II

- As work proceeds on conceptual analysis, continue open dialog between DAA, User Representative, Program Manager, and new players as they are identified
- Expect give-and-take among all parties as federation scenario, federation objects, federation relationships, etc. are defined
- Modify the SSAA so it is kept current as details of the federation emerge
- Make sure all parties agree to SSAA modifications / additions

FSP Phase III

- Keep all parties talking. Make sure security representatives are aware of all meetings and meeting outcomes. If they could be present, it would be better as they can provide immediate feedback
- As federates are identified and finalized, ensure all previous decisions and documentation in SSAA are agreeable to all parties. This is a decision point for federate inclusion in federation.
- Data is often the key in security - this is where data to be exchanged is defined
- Keep SSAA current

FSP Phase IV

- Since security personnel have been involved, the tests for certification may be the same tests used (in whole or in part) for federation integration
- Types of certifications achievable (for both federation and federation execution: unconditional, unconditional with identified risks, conditional on modifications, denied
- Modifications to federation are decision of DAA, User Representatives, and Program Manager
- If certification not achieved, Federation Execution cannot proceed

FSP Phase V

- Execution proceeds in secure manner
- Tight configuration control is essential to maintaining accreditation posture
- System modifications may require re-accreditation, and should not be taken lightly
- Once federation is dissolved, accreditation is invalid unless it was achieved for federation. Re-emergence of federation requires reaccreditation
- SSAA becomes repository for all security decisions, etc. and should be put in repository for lessons learned.

Summary

- Goal is accreditation and secure use of federation - not a guarantee
- Goes hand-in-hand with FEDEP
- Expected to work for:
  - geographically distributed and locally contained federations
  - Single or multi-domain federations
- What is lacking?
  - Experience in the process (counting on your feedback)
  - Need to spread the word (especially to accreditors who may be inexperienced in HLA)

Next Steps for FSP

- C&A Process
  - Incorporate comments
  - Provide to AMG for their comments - incorporate as necessary
  - Continue to brief concept as requested; incorporate comments as necessary
  - Research security C&A tools to assist federation managers in C&A'ing their federation; provide in C&A process

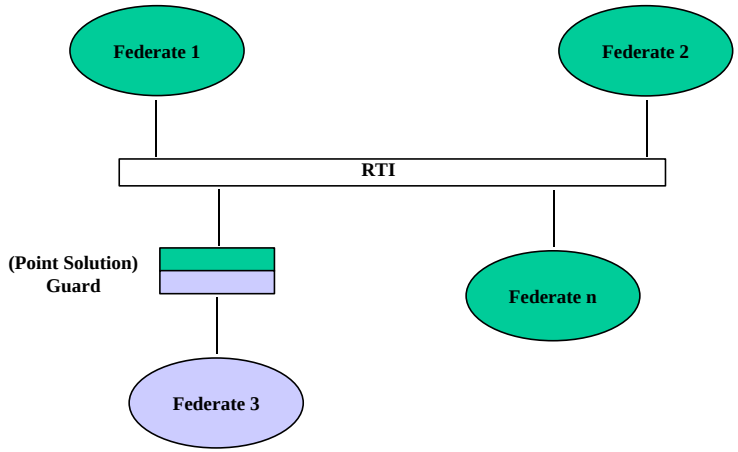
HLA Runtime Security Arch

- 3 modes of operation
  - Near term - system high operations
  - Mid term - enclaves for each security level
  - Long Term - Multi-level Security

Near Term HLA Security Arch

- Characterized by a single security level for data exchange
- Routine - this is current mode of operation for most federations
  - May not be the most practical way to accomplish federating
- Possibly requires federates to add h/w, s/w, and/or procedures to modify their federate outputs

Near-term Sec Arch (example)



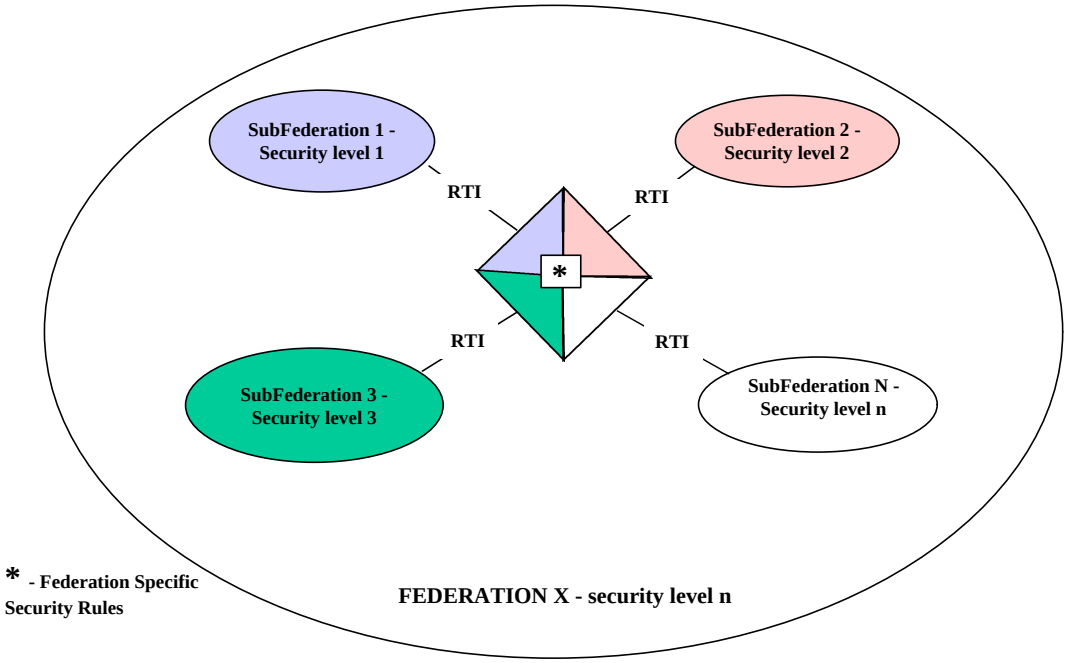
Mid Term HLA Security Arch

- Concentrating program effort in this area
- Allows multiple levels of security (each as its own enclave) within a federation
- Utilizes Digital Security Guard (specialized functionality of a Bridge Federate) capability to link enclaves together - 2 parts
  - Mechanism - goal is to accredit this
  - Security Policy Parameters - federation specific

Mid Term HLA Security Arch

- TIS provided initial investigation
  - "discovered" general functionality for linking multiple federations together (bridge federate)
- SAIC prototyped bridge federate and wrote specification - SEI examined for completeness
- Bridge Federate Specification underwent security feasibility assessment
  - Is this functionality a guard would normally provide
  - Is this C&A'able; under what circumstances?

Mid Term HLA Security Arch



Multi-Domain Sec Arch Rpt

- 3 Main parts:
  - Guard Technology Survey
  - Is Guard Federate subclass of Bridge Federate?
  - Accreditation Issues

Practical Assumptions

- Federates themselves assumed to operate System High
- Federates operate in System High Federations
- Determining what objects can be shared across security domains (federates) is difficult
- Accreditation of Multi-Domain Security Federations is still an unknown

Guard Characteristic

- Manual bi-directional
  - Requires operator intervention
- Automated low-to-high
  - Permits only uphill flow, through high assurance h/w and s/w
- Automated bi-directional
  - Permits flow in both directions; but limits flexibility of data it can accommodate

Bridge Federate/Guard Federate

- Bridge federate is a unit that joins two or more federations
- MAC semantics considered for RTI service groups (excluding TM and DDM - under work now)
  - Attribute Ownership Divestiture complicated; suggestion is to disallow this function

Accreditation Issues

- There is no precedent for accrediting sets of federations united by bridge federates as guards
- Use of a guard actually decreases level of accreditation needed by federation
  - Problem is shifted
- Issues exist with
  - Interconnection
  - Trusted platforms
  - Covert channels

Bridge/Guard Study Conclusions

- Accreditation of the bridge federate between two federations is within current state of the art
- Bridge federate must understand and transport MAC labels
- Accrediting a federation connected to a bridge federate may require retesting individual federates
- A covert channel analysis of the federation may be necessary

Long Term HLA Security Arch

- Involves Multi-level Security
- General MLS technology considered to be in its infancy
- Work considered to be beyond the scope of DMSO efforts

Next Steps (cont'd)

- Feasibility study of HLA Security Architecture - depends on results
  - COMPLETE study of TM and DDM
  - Option 1 - consider DMSO work completed and let implementers use specifications as needed
  - Option 2 - improve bridge federate specification so it is formalized (recommended)
  - Option 3 - Work to identify a potential partner for some prototyping experience
  - Option 4 - Build it (not recommended)