SPPF & SOAP Security

- Framework draft – connection oriented, session HTTPS + digest authentication
- SOAP draft – SOAP over HTTPS with digest authentication
- Batch requires message security vs. transport security
- Actors SPPF batch user cases
  - Registrant - acting in the batch commands
  - Session client - provides the batch upload
  - Registry
- Threats
  - Malicious XML Document
    - Authorized client, Illegitimate registrant - posts malicious batch request XML document
    - Legitimate registrant - possible Zombie - posts malicious XML document

Malicious SOAP Documents

- XML Parsing DOS
  - Coercive Parsing
  - Oversize Payload
- SPPF behavioral DOS on registry
  - Table scan queries
  - Massive inserts
  - Massive roll back at end of long batch
    - Stop and Roll-Back see SOAP Draft
    - http://tools.ietf.org/html/draft-ietf-drinks-spp-protocol-over-soap-01#section-6.2.5
- produces resource starvation of the registry
    - http://tools.ietf.org/html/rfc4732#page-5
    - https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet
    - http://msdn.microsoft.com/en-us/library/ff650168.aspx

Defenses

- Authenticate Registrant - message security
  - Require XML Signatures WS-SECURITY [WS-I Basic Security Profile]
    - http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html
    - File level
    - Block level
  - However - WS-Security - high overhead
    - Streaming Processing of WS-Security
      - http://www.sundaychennai.com/dotnet_iee2011/Server-Side%20Streaming%20Processing%20of%20WS-Security.pdf
- Application Level Gateways / WS Firewall
  - Schema Validation
    - http://www.mendeley.com/research/protecting-web-services-dos-attacks-soap-message-validation/

SPPF Specific Defenses

- Deep Inspection
  - Analysis of batch file before processing
- Behavioral Analysis
  - Do these commands make sense for this registrant
  - Do the commands make sense in sequence
  - Do the commands make sense given this registrants command history
- Resource Cost Scrip
  - Assign a cost to each command
  - Registrants get a “budget”
    - http://www.cs.columbia.edu/~angelos/Papers/sosmp.pdf

Implications for SPPF SOAP and Batch

- Batch processing use cases not covered in use case draft
  - Failure modes
  - Security considerations
- Still maintain should be a separate protocol draft