Web Services Cyber-Security Issues

Debby Quock

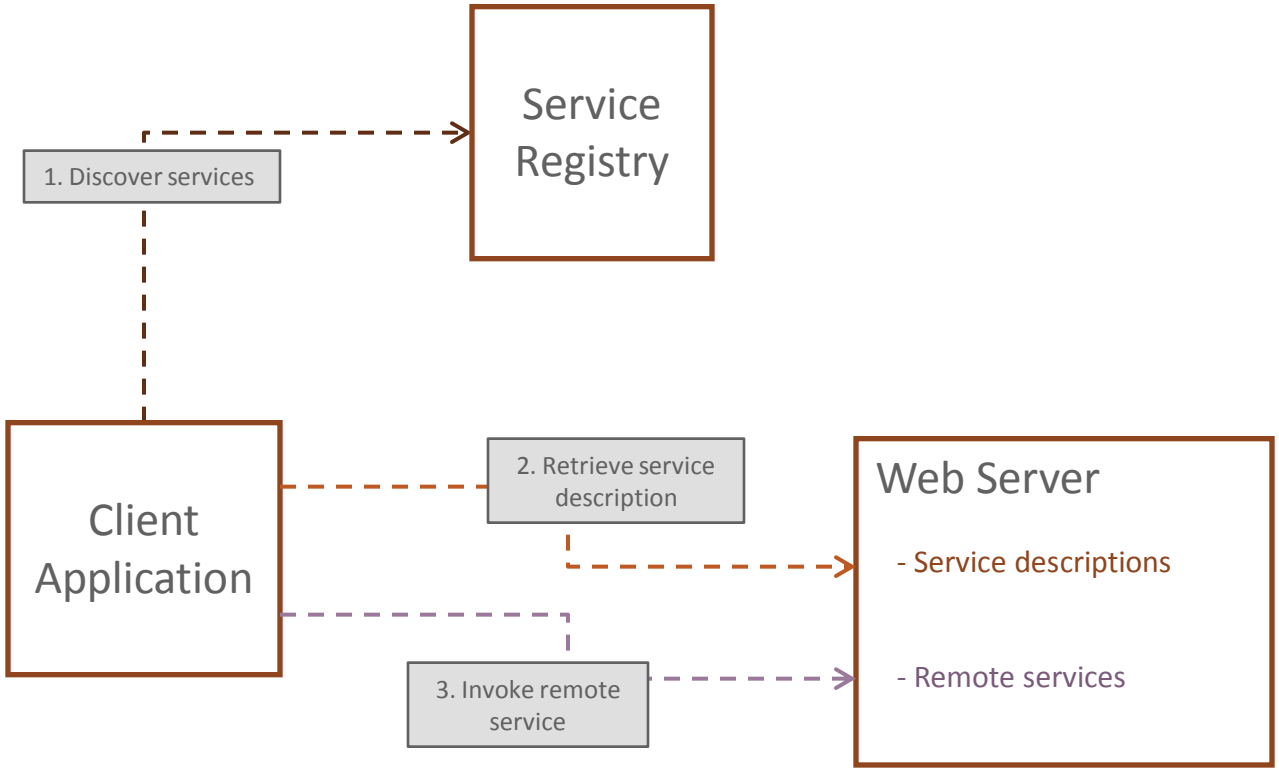
Advanced Photon Source

Overview:
Web Services and Their Cyber-Security Issues

- Basics of Web Services
- Example at the Advanced Photon Source
- Cyber-Security Issues
- Cyber-Security Standards
- Cyber-Security Organizations
- Cyber-Security Design Practices
- Summary

Web Services Basics

- How it works



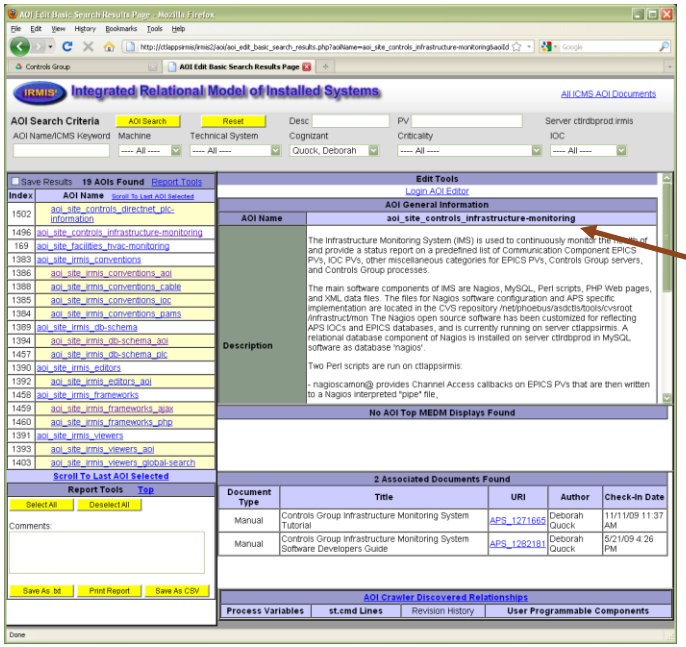
Web Services Basics

- Service-Oriented Architecture (SOA) protocol stack

Architectural Layer	Web Services Standards
Business Workflow	BPEL WSCI
Web Services	UDDI WSDL
Communications SOAP (RESTful)	XML
Client-Server Transports HTTP SSL TCP/IP	

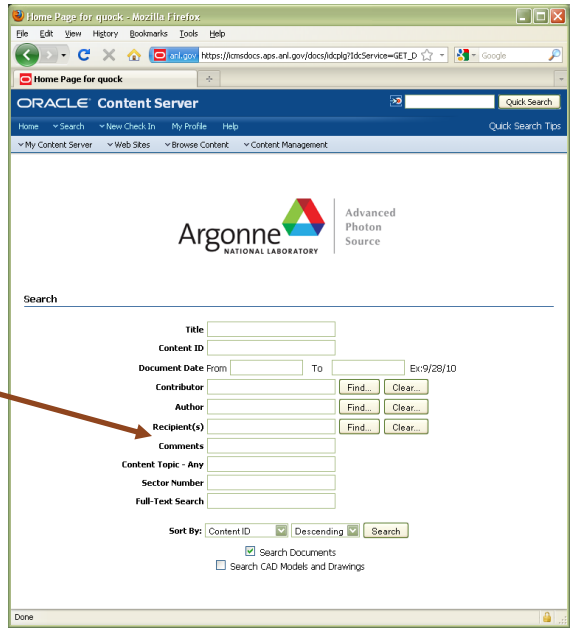
Web Services at the Advanced Photon Source

IRMIS (Integrated Relational Model of Installed Systems)



SOAP
Web Services

Oracle Content Server



IRMIS PHP Application

```
...
$client = new SoapClient($wsdl,
                array('login'=>$user_name,'password'=>$user_password));
...
$param = array("queryText"=>$searchString,"sortField"=>"dInDate");
$retVal = $client->AdvancedSearch($param);
$search_results = $retVal->AdvancedSearchResult->SearchResults;
```

Oracle Content Server WSDL

https://icmsdocs.aps.anl.gov/docs/idcplg?
IdcService=DISPLAY_URL&dDocName=SEARCH

Web Services Cyber-Security Issues

- The software used to manage Web services is complex
- The boundaries of communication may extend outside of an organization's intranet
- Dynamic reconfiguration of a client application can be easily obtained through both combination and reuse of individual Web services
- Web services security threats:
  - message alteration
  - message reading
  - man-in-the-middle attack
  - principal spoofing
  - forged claims
  - message replay
  - denial of service

Web Services Cyber-Security Standards

- Security Assertion Markup Language (SAML)
  - Defines authentication and authorization assertions
  - SAML assertions can be included in the header or in the payload of a SOAP message

- WS-*
  - Refers to a family of Web services standards supported by various organizations
  - WS-Security

    Defines security tokens that can be used for claims of authentication or proof of some right
  - WS-ReliableMessaging

    Describes a protocol that allows SOAP messages to be reliably delivered between distributed applications in the presence of software component, system, or network failures

Web Services Cyber-Security Organizations

- Organization for the Advancement of Structured Information Standards (OASIS)
  - Not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society
  - Produces more Web services standards than any other organization
  - Sponsors ebXML (Electronic Business using eXtensible Markup Language), a modular suite of specifications

- World Wide Web Consortium (W3C)
  - International community where member organizations, a full-time staff, and the public work together to develop Web standards
  - Among the many standards developed and supported by W3C are XML Encryption and XML Signature

Web Services Cyber-Security Design Practices

Software development life cycle:

- Security requirements
- Security architecture
- Web services security standards
- Certification
- Run-time security monitoring
- Penetration testing

Analysis software products examine:

- Conformance validation
- Integrity checks
- XML schema validation
- XML encryption
- XML signature
- WS-Security
- User authentication
- Audit
- Alert
- Web services access control

Conclusion

- The complex nature of Service-Oriented Architecture applications calls for governance of SOA and its underlying Web services technology.
- Cooperation among industry and Web services standards organizations is crucial to ensure reliable Internet-based business and government processes, and safeguarding of intellectual property and high-security-level government data.
- Web services standards organizations are well established and have received widespread support and contributions from major computer and IT corporations.
- At Argonne National Laboratory, Web services applications have been deployed successfully by joining and making more efficient use of disparate software applications.
- Web services will continue to grow in usage in industry and government institutions, and thus the need for ever-improving Web services cyber-security measures will grow as well.