NIIIP SPARS

A Case Study in Secure Architectures for e-Business

Paul Horstmann, John Laurentiev, John Schuetz.

IBM/NIIIP, B/010, P/103, Poughkeepsie, NY

Horstman@us.ibm.com, laurentj@us.ibm.com, schuetz@us.ibm.com

Introduction/Agenda

- NIIIP
  - National Industrial Information Infrastructure Protocols (NIIIP) Consortium
- Projects
  - NIIIP Project (1994-1998)
    - C++/SOM/DSOM/X-Windows
  - NIIIP SPARS (1998-2001)
    - Java/RMI-IIOP/Java Client
  - NIIIP SPARS-SC (2001-2003)
    - Java/HTTPS/DHTML
- The Future

NIIIP

- Ad Tech Program
- Broad array of participants (users, vendors, universities)
- Focus on Engineering
- UNIX/C++/X-Windows
- Distributed Objects - CORBA(SOM/DSOM)
- Limited security focus, some DCE, early PKI and secure webservers (SHTTP)

NIIIP Lessons Learned

- Distributed Objects is a Complicated Technology
  - Object trust and authentication issues not addressed
- No one (yet) worrying about firewalls
- Interoperability (much less security) across different ORBS severely limited

SPARS

- Deployment Program into production
- U.S. Shipyards, Suppliers
- Focus on Purchasing, Contract Management
- At start: Windows/C++/CORBA (Component Broker)
- At end: Windows/Java/Application Server (EJB) (RMI/IIOP)
- Security driven by US Navy (NAVSEA)

SPARS Security

- US Navy largest customer
  - Drives security, encryption requirements
  - Limited classification levels supported (technical data)
- Large number of suppliers (thousands)
- Java Applet/Application desktop
  - IIOP causes firewall pain
  - Secure Tunnel (FIPS 140-1) protects RMI/IIOP
  - Object Security externalized (LDAP)

Secure Tunnel Details

- Creates a virtual Socks and/or X-windows proxy spanning as many as two firewalls.
- Both end "Proxies" are authenticated to one another using X.509 certificates.
- The end proxies connect to a middle proxy that can be reached by both parties.
- The end proxies negotiate a TLS session through the middle proxy.
  - Once the TLS session is established the data is never in the clear between the end proxies.

SPARS Lessons Learned

- Every Supplier has a different firewall technology
- Every supplier runs a different version of Windows, et al
- Customer required data checking -> Fat Applet
- Fat Applet -> Application, distributed with Tunnel Client
- Joys of distributing an installation disk/process
- Net: Worked well but a bear to support

SPARS Thin Client/VES Security

- Three Tier Architecture
  - Outer Webserver - locked down ports
  - Inner Application Server
  - Separate Data Server
    - Backup, Physical Control of data access

SPARS-SC

- Deployment Program
- Shipyards <-> Supplier e-Business
- US Navy Data Security Requirements
  - Secure Interactions (transmission of data)
  - Mulit-level data classifications - additional levels supported (NNPI/NOFORN)
  - Looooooong shelf life - how to migrate/archive data

US Navy Data Classifications

- NNPI - Naval Nuclear Propulsion Information
  - Documents (or screens) containing NNPI information must be marked.
  - No access by foreign nationals permitted (NOFORN).
  - Encryption must be handled by FIPS 140-1 approved cipher modules.
- The business processes implemented in the VES address Unclassified NNPI data.

SPARS-SC Security

- HTTPS
  - Standard OK for low-security data
  - FIPS 140-1 for NNPI/NOFORN
  - Physical Security (location of servers) as issue
- Data instances stored as Entity Beans
- Externalized security (DB/2) per instance
  - Supported both EJB and non-EJB access
- Externalized User/Group/Role structure in LDAP with separate User Registry Interface
- MOM-based legacy system integration

SPARS-SC Lessons Learned

- Thin Client easier to install/support
- Thin Client functional additions
  - Data encryption at client end
  - Digital Signatures
- Web Services/MOM limiting cross-enterprise IIOP use

The Future

- Web Services
  - Distributed Functions
  - Dynamically configured systems
- Distributed Security Models
- Enhanced focus on encryption
- Enhanced focus on Digital Signatures