

Security Expert Group

Christopher Steel



Expert Group Members

- Chris Steel – Sun Microsystems
- Guy Beiber – Motorola
- Sue Haines – DERA
- Ayal Spitz – Mitre Corp



Framework Objectives

- Service developers not burdened with authentication
- Access control independent of authentication
- Centralized user management
 - Federated domains
 - Role based access control
- PKI architecture



Creating a Security Framework

- Determine requirements
- Establish policies
- Leverage existing security technologies and implementations
 - Java™ 2 platform
 - Java™ Authentication and Authorization Service API
 - Java™ Secure Socket Extension
 - Java Naming and Directory Interface™



Methodology

- Goals / Requirements
- Use Cases
- Architecture
- Interfaces
- Tools / Utilities
- Examples



Goals / Requirements

- Security Services shall support configurable security for many domains including: commercial, military, and international systems.
- Security Services shall support use across Multiple Security Levels.
- The Security Services shall be in alignment with the Common Criteria and ARS 380-19
- Security Services shall provide code, transport, and service security.
- Security Services shall provide authentication of users and executables.
- Security Services shall provide for configuration of authorization.



Goals / Requirements (cont)

- Code Security shall enforce system access control.
- Service Security shall enforce service access control.
- Transport Security shall provide data confidentiality and integrity.
- Security Services shall provide non-repudiation.
- Security Services shall provide auditing.
- Security Services shall provide configurable attack detection.
- Security Services shall provide configurable attack counter measures.



Use Cases

- HQ Example
- M-commerce Example
- Home
- Digital Environment
- Military
- Authentication and Authorization of New User



HQ Example

- New HQ staff member should be able to
 - Connect into the CIS network at any location.
 - Setup the machine by installing a single 'lightweight' Java application which
 - Provides access to the Dynamic Clients available within the OpenWings environment
 - Provides an appropriate authentication token.
- Once complete the officer should be able to
 - Select any service types that are appropriate for their role.
 - Have their machine automatically updated to access them.
 - Locate and utilize any service needed to perform their role.
 - Automatically reconnected to an equivalent service.
- The network itself should be able to
 - Reconfigure in times of stress.
 - Self-repair and automatically restore clients / services.
- Clients should be able
 - Register an interest in specific events (such as certain data sources becoming available) and be automatically informed if these occur.



M-Commerce Example

- Upon entering a store, a user goes pulls out their wirelessly enabled pocket PC (with Bluetooth for instance).
- The store has published services that are available to anyone, which show up as a web page for the user.
- The user selects the item locator service, that shows a store map and allows them to enter a product category and it shows up on the store map.
- The store has an optional service, which is a Bluetooth enabled bar code scanner.
- This device shows up as a service on the users handheld, which scans in items they show up on their handheld device with a running total.
- The user gets to the checkout and uses the buy service, which takes his selected items and sends them to the cashier.
- The user then selects a payment method and a secure transaction takes place that lets the purchase go through.
- The user's handheld then securely connects back to their home accounting service (quicken) and notifies other family members devices of the reduction in available funds.



Home Example

- A home PC is connected with broadband access using a firewall / router.
- The user hosts many personal services on this machine that are available to any network appliance in the house.
- The house has some wired networking and wireless networking that allows discover of mobile devices in the house.
- The user can also, key his personal devices, such as phones and PDAs to access their home services anywhere they can get a network connection.
- Visitors to the home can be granted access to various home services in the guest role. This includes light control, internet access, television control, etc.

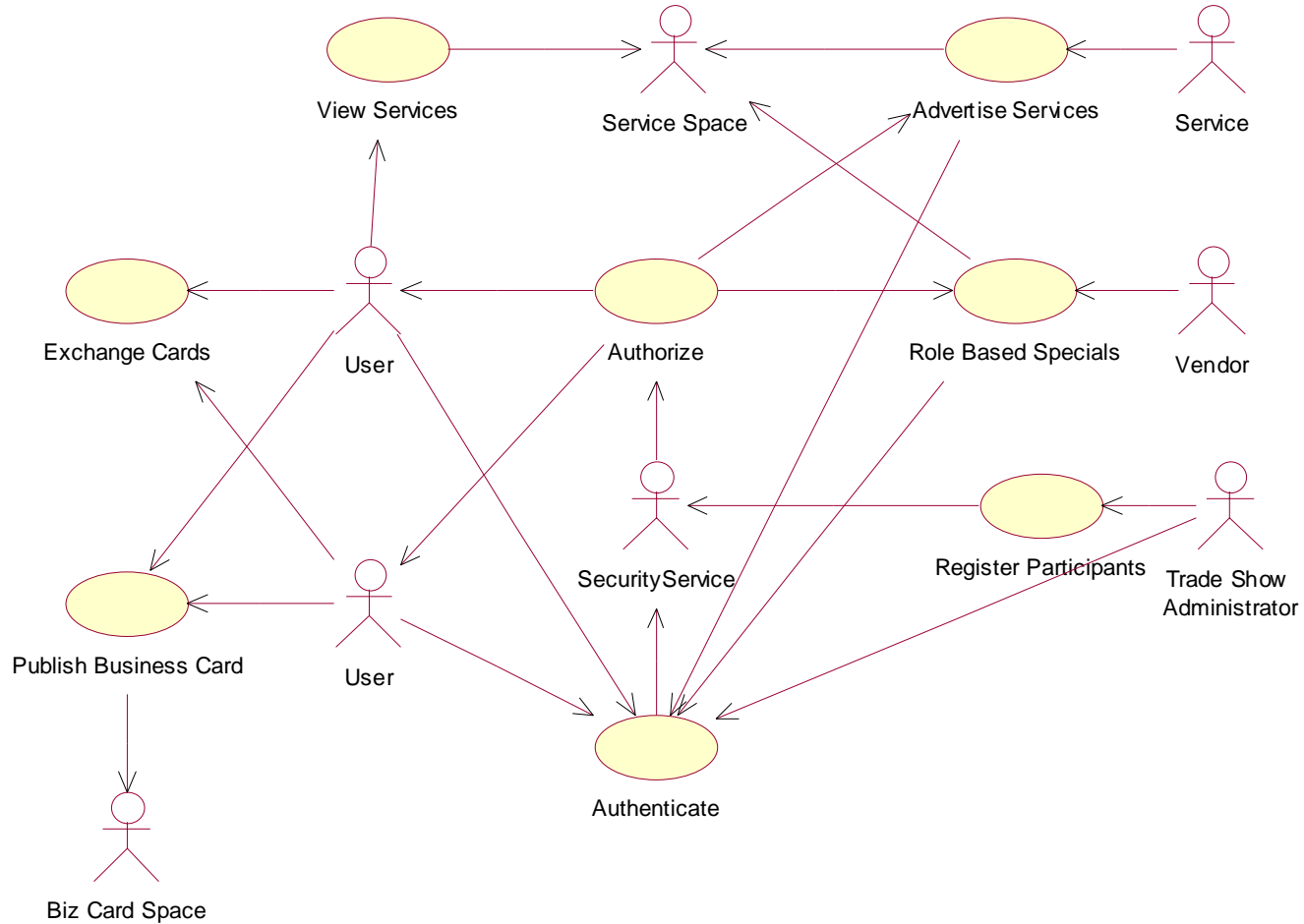


Digital Environment Example

- A large trade show is being held and has been wirelessly enabled.
- As users go around the show floor the various vendor services show up on handheld computing devices.
- Some of these services are simply web pages, some are standalone demos, and some are interactive demos where many conference attendees are participating.
- In addition, many people have chosen to publish their business cards and there are exchanged in real time at the show.
- Vendors also advertise special services and discounts for partner companies.
- Users should be able to securely access vendor's services.
- Users will be authenticated and authorized
- Discounts will be provided based on user roles



Digital Environment Use Case



Military Example

- A Tactical Operations Center (TOC) is being formed.
- As systems drive up and are connected the services of these systems become part of the TOC by forming a relationship with the existing TOC.
- Capabilities throughout the TOC are accessed thru various roles.
- Collateral staff is allowed access to a more limited roll that gives them the basic battlefield knowledge to work with the national military.



Authentication and Authorization of New User Example

- A new user registers in a central directory service.
- User is then able to walk up to an existing compute resource and authenticate and authorize themselves to any of the existing services in the enclave.
- User should be able to select from one or more available roles, depending on the ability of the resource to support the authentication mechanism required by that role (i.e. smart card or biometric device support).
- Once authenticated for a particular role, the user should be able to access the services available to that particular role with bi-directional authentication and authorization support and with appropriate levels of confidentiality as necessary.



Architecture

- Identify security commonality in use cases
- Develop high level architecture
- Iterate on architecture

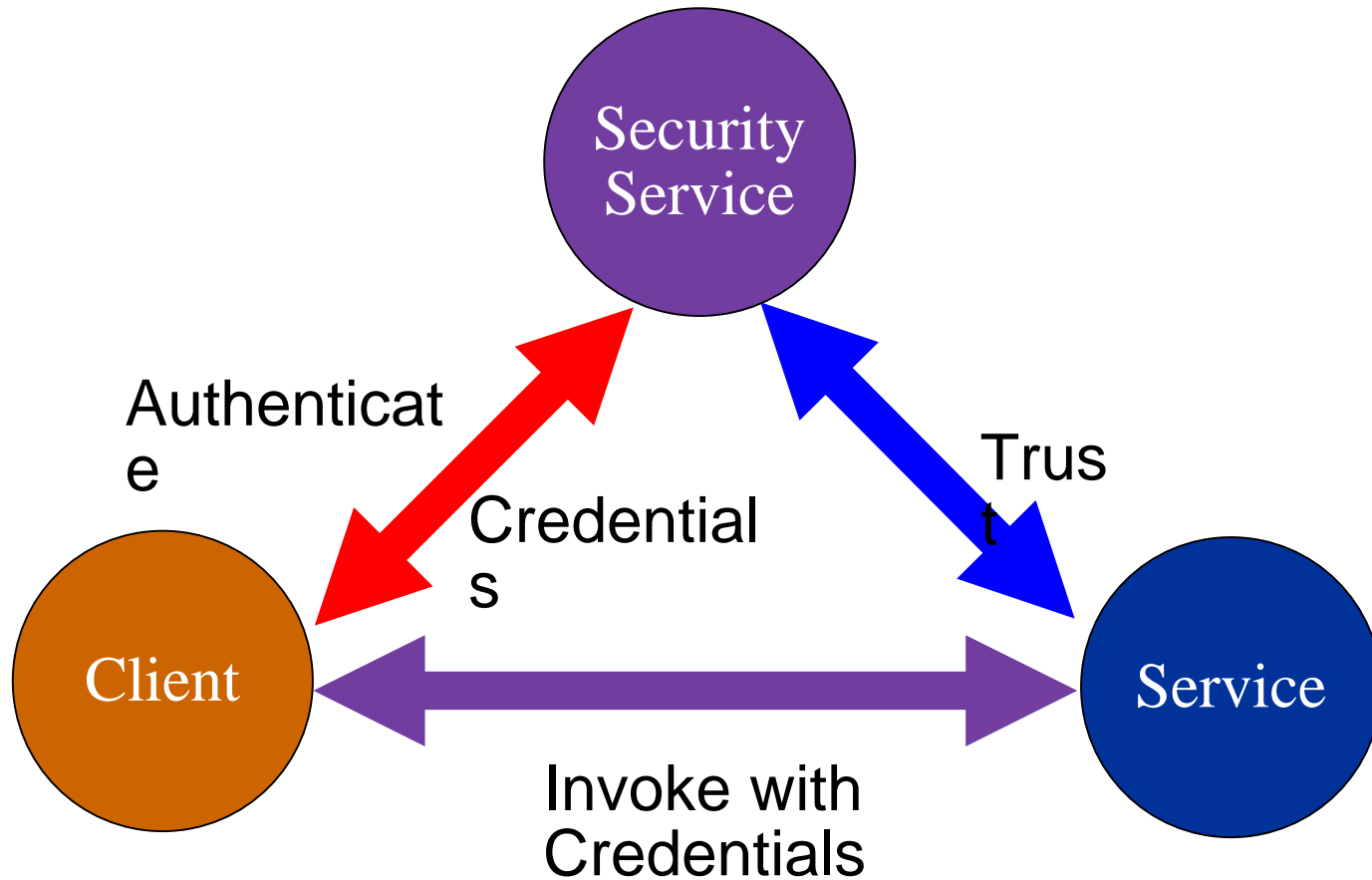


Trusted Third Party Authentication

- Central authority authenticates clients
- Provides centralized user management
- May act as high level CA
- Maintains repository of access control information



Security Service Model



RMI Security Status

- JSRs 76 and 78 rejected
- RMI security being rolled into Jini namespace
- Implementation to follow Merlin release



Next Steps

- Complete Use Cases
- Create Sample Approach
- Define Interfaces
- Identify and Describe Supporting Tools and Utilities



Q&A





Thanks!

