Java is a trademark of Sun Microsystems, Inc.

JavaOne℠

Java™ Card Platform Puzzlers

Alexander Glasman,
Hema Kalsi, Thierry Violleau,
Lichun Zhan

Sun Microsystems, Inc.

At the cross-road of all Java Platforms...

- Features from All Java Platforms ...
  - Java Platform, Micro Edition
  - Java Platform, Standard Edition
  - Java Platform, Enterprise Edition
- coming to Smart Card Applications in
    - Java Card 3.0 Platform

Why Puzzles?

- Show specifics of Java Card 3.0 Platform
- Entertain You
- Show Practical Recipes

>

Puzzlers List

- Persistence
- Transaction
- Sharing
- Deletion
- Secure Hosting
- Permission
- Authorization
- Authentication

Persistence Puzzle

```
public class PersistencePuzzle extends HttpServlet {
   public static int staticValue = 5;
   public int instanceValue = 10;
}
```

- What will be the sum of these fields after card reset?
  - A - 0
  - B - 5
  - C – 10
  - D – 15
  - E – Other

Volatility Vs. Persistence

- Volatile Objects
  - Garbage Collected on card tear (reset)
  - All newly created objects are volatile
- Persistent Objects
  - Retain its content across a reset
  - Need to be promoted to become persistent
- Persistence by Reachability Principle
  - Persistence according to reachability from an object that acts as its root of persistence

Persistence by Reachability Principle

- Reachability Disrupting Objects
  - Transient array object of type Object
  - Instances of TransientReference class
- Roots of persistence
  - Static Fields
  - Web Application Model
    - javax.servlet.ServletContext
  - APDU Application Model
    - javacard.framework.Applet

Servlet & Persistence

- MUST be persistent
  - Servlet Context
  - Filters and Listeners
  - Load-on-startup servlet
- MAY be volatile
  - Servlets not configured as load-on-startup

Persistence Puzzle Answer

```
public class PersistencePuzzle extends HttpServlet {
   public static int staticValue = 5;
   public int instanceValue = 10;
}
```

- What will be the sum of these fields after card reset?
  - A - 0
  - B - 5
  - C – 10
  - D – 15
  - E – Other

Persistence Puzzle Answer

```
public class PersistencePuzzle extends HttpServlet {
    public static int staticValue = 5;
    public int instanceValue = 10;
}
```

- What will be the sum of these fields after card reset?
  - ~~A - 0~~
  - B - 5
  - C – 10
  - D – 15
  - E – Other

Persistence Puzzle Answer

```
public class PersistencePuzzle extends HttpServlet {
   public static int staticValue = 5;
   public int instanceValue = 10;
}
```

- What will be the sum of these fields after card reset?
  - ~~A - 0~~
  - B - 5
  - ~~C – 10~~
  - D – 15
  - E – Other

Persistence Puzzle Answer

```
public class PersistencePuzzle extends HttpServlet {
   public static int staticValue = 5;
   public int instanceValue = 10;
}
```

> What will be the sum of these fields after card reset?

- ~~A - 0~~
- B - 5
- ~~C – 10~~
- ~~D – 15~~ – only for load-on-startup servlets
- E – Other

Persistence Puzzle Answer

```
public class PersistencePuzzle extends HttpServlet {
    public static int staticValue = 5;
    public int instanceValue = 10;
}
```

- What will be the sum of these fields after card reset?
    - ~~A - 0~~
    - ~~B – 5~~ – implementation specific
    - ~~C – 10~~
    - ~~D – 15~~ – only for load-on-startup servlets
    - E – Other

Persistence Puzzle Lesson

- Do not rely on persistence of servlets not configured as load-on-startup!
  - It's implementation specific

Transaction Puzzle Source

```
private static int staticValue = 5;
private TransientReference<Integer> instanceValue =
    new TransientReference<Integer> (new
  Integer(10));

@TransactionType(TransactionTypeValue.REQUIRES_NEW)
protected void checkTransaction() throws Exception {
    staticValue += 1;
    instanceValue.set(new Integer(15));
    throw new Exception("Exception from
  Transaction");
}
```

Transaction Puzzle

- What will be the sum of these two values after invocation of checkTransaction?
  - A - 15
  - B - 16
  - C – 20
  - D - 21
  - E - Other

Transaction Facility

- Atomicity
  - All or None
- Consistency
  - Consistent state before the start and after the end
  - Isolation is not supported
- Durability
  - Updates are committed when transaction is successfully completed

Transaction Demarcation

- @TransactionType annotation
  - MANDATORY, REQUIRED, REQUIRES_NEW, SUPPORTS, NOT_SUPPORTED, NEVER
- Class-level or Method-level
- Default Type
  - SUPPORTS
- Constructors and Static Initializers do not support
  - NOT_SUPPORTED behavior

Reachability Disrupting Objects and Transactions

- Transient Arrays
  - Components are not conditionally updated
  - Updates are committed immediately
- TransientReference
  - Private reference field is not conditionally updated
  - Update is committed immediately

Transaction Puzzle Answer

- What will be the sum of these two values after invocation of checkTransaction?
  - A - 15
  - B - 16
  - C – 20
  - D - 21
  - E - Other

Transaction Puzzle Answer

- What will be the sum of these two values after invocation of checkTransaction?
    - A - 15
    - ~~B - 16~~
    - C – 20
    - ~~D - 21~~
    - E - Other

Transaction Puzzle Answer

- What will be the sum of these two values after invocation of checkTransaction?
  - ~~A – 15~~ – value of TransientReference is not rolled back
  - ~~B - 16~~
  - C – 20
  - ~~D - 21~~
  - E - Other

Transaction Puzzle Answer

> What will be the sum of these two values after invocation of checkTransaction?

- ~~A – 15~~ – value of TransientReference is not rolled back
- ~~B - 16~~
- C – 20
- ~~D - 21~~
- ~~E - Other~~

Transaction Puzzle Lesson

- Do not use transient objects in transactions.

Sharing Puzzle Sources

```java
public interface ServiceSI extends Shareable {
     int getIntValue();
     String getStringValue();
}
```

```java
// Provider Application
public class ServiceSIO implements ServiceSI {
    public int getIntValue() { return 10; }
        public String getStringValue() {
              return String.valueOf(10);
        }
}
```

```java
// Client Application
         int intValue = puzzleService.getIntValue();
         String strValue = puzzleService.getStringValue();
         int result = intValue + Integer.parseInt(strValue);
```

Sharing Puzzle

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - A – result is 10
  - B – NullPointerException is thrown
  - C – result is 20
  - D – intValue is 10; strValue is “10”

Inter-Application Communication

- Context Isolation
  - Application Firewall
  - Object Ownership and Access
  - An object can ONLY be accessed by its owing context
  - SecurityException when access is disallowed
- Shareable Interface Object-based Services
  - Applications define and register SIO-based services
  - Application can lookup SIO-based services registered by other applications

Object Ownership Transfer Mechanism

- Allows transfer of object ownership to other applications
- Transferable Classes
  - Implicitly Transferable
    - Instances are not bound to any context
    - Boolean, Byte, Character, Integer, Long, Short
    - Class, Throwable and API-defined subclasses
    - String (literal strings, interned String objects)
  - Explicitly Transferable
    - String (newly created, computed at runtime)
    - Arrays

Sharing Puzzle Answer

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - A – result is 10
  - B – NullPointerException is thrown
  - C – result is 20
  - D – intValue is 10; strValue is “10”

Sharing Puzzle Answer

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - A – result is 10
  - ~~B – NullPointerException is thrown~~
  - C – result is 20
  - D – intValue is 10; strValue is “10”

Sharing Puzzle Answer

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - ~~A – result is 10~~
  - ~~B – NullPointerException is thrown~~
  - C – result is 20
  - D – intValue is 10; strValue is “10”

Sharing Puzzle Answer

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - ~~A – result is 10~~
  - ~~B – NullPointerException is thrown~~
  - C – result is 20
  - D – intValue is 10; strValue is “10”

Sharing Puzzle Answer

- Provider application - Registered service
- Client application
  - Successfully got the service puzzleService
  - Executed the cited code
- Which of the following statements is true?
  - ~~A – result is 10~~
  - ~~B – NullPointerException is thrown~~
  - ~~C – result is 20~~ – SecurityException is thrown
  - D – intValue is 10; strValue is “10”

Sharing Puzzle Lesson

- SecurityException will be thrown on the attempt to access object not from current context

Deletion Puzzle Sources

```
// Extension Library
public class DeletionLib {
      public static Object objValue = new Object();
}
```

```
// Main Application
public class MainApp extends HttpServlet {
      public Object objFromLib =
        DeletionLib.objValue;
}
```

Deletion Puzzle

- Load extension library
- Run the main application
- Try to delete and unload the main application
- What will be the result of this attempt?
  - A – Successfully deleted and unloaded
  - B – Deleted, but the unloading operation fails
  - C – The deletion operation fails
  - D - Other

Deletion of Application Instance

- ALL Objects owned by the Application – Inaccessible on the Card
- Dependency check
    - No references to ANY objects owned by the Application from other entities

Mutual-Dependencies Threat

- The extension library has dependency on the main application
  - The main application is the first one accessing the DeletionLib library
  - DeletionLib.objValue is created in the context of the main application
- The main application has dependency on the extension library

Deletion Puzzle Answer

- Load extension library
- Run the main application
- Try to delete and unload the main application
- What will be the result of this attempt?
  - A – Successfully deleted and unloaded
  - B – Deleted, but the unloading operation fails
  - C – The deletion operation fails due to dependency
  - D - Other

Deletion Puzzle Answer

- Load extension library
- Run the main application
- Try to delete and unload the main application
- What will be the result of this attempt?
  - ~~A – Successfully deleted and unloaded~~
  - ~~B – Deleted, but the unloading operation fails~~
  - C – The deletion operation fails due to dependency
  - ~~D - Other~~

Deletion Puzzle Lesson

- Use of static fields in extension library can block the deletion of application using this library
  - Deleting the library can not be done without unloading the library at the same time

Secure Hosting Puzzle

- Runtime descriptor of application has:
  - Web-Secure-Access-Only: false
- Deployment descriptor has the transport-guarantee attribute set as CONFIDENTIAL
- The Java Card platform will host the web app on?
  - A – http://localhost:default-plain-port
  - B – http://localhost:secure-port
  - C - https://localhost:default-plain-port
  - D - https://localhost:secure-port

Secure Hosting of Web Application

- Web Application is hosted on dedicated secure host if
  - Has requirements for transport guarantee in deployment descriptor
    - Content Integrity (INTEGRAL)
    - Content Confidentiality (CONFIDENTIAL)
  - Has requirements for exclusive secure access in runtime descriptor
    - Web-Secure-Access-Only = true

Secure Port Determination

- Static Port Allocation
  - Requirement for Secure Port in runtime descriptor
  - Web-Secure-Port-Number: <port #>
- Dynamic Port Allocation
  - No Requirement for Secure Port

Port-Based Virtual Hosting

- Exclusively on the Default Plain Port
  - No Requirements for Secure Hosting
  - Requirement for Secure Port is ignored
- Exclusively on a Dedicated Secure Port
  - Requirement for Exclusive Secure Access
- Protected Content - Dedicated Secure Port, Unprotected Content - Default Plain Port
  - Only transport guarantee requirements
  - Unprotected content is equally serviced on both ports

Secure Hosting Puzzle Answer

- Runtime descriptor of application has:
  - Web-Secure-Access-Only: false
- Deployment descriptor has the transport-guarantee attribute set as CONFIDENTIAL
- The Java Card platform will host the web app on?
  - A – http://localhost:default-plain-port
  - B – http://localhost:secure-port
  - C - https://localhost:default-plain-port
  - D - https://localhost:secure-port

Secure Hosting Puzzle Lesson

- A web application that has requirements for content integrity or confidentiality needs to declare at least one user data security constraint with a transport guarantee value of INTEGRAL or CONFIDENTIAL in its web application deployment descriptor.
- A web application may also define Web-Secure-Access-Only attribute as true in its runtime descriptor for exclusive secure access of all its content.

Permission Puzzle Source

```
InputStream is = null;
HttpConnection hc = null;
try {
        hc = (HttpConnection)Connector.open("http://www.sun.com");
        is = hc.openInputStream();
        out.println("No exception");
}catch(SecurityException e){
        out.println("AccessControlException--"+e);
}catch(Exception e){
        out.println("Other exception--"+e);
}
```

Permission Puzzle

- With only following permission granted in the application protection domain:
  - javacardx.io.ConnectorPermission "https://*/*", "connect,listen,accept,read,write"
- What will happen when build the connection?
  - A - No exception
  - B - AccessControlException
  - C - Other exception
  - D - Other

Permission

- Protect resources
  - Security-sensitive system resources
  - Application resources
- Permission Objects are created when load and/or update:
  - Platform security policy
  - Card management security policy

Protection Domain

- A set of permissions granted to an application or group of applications.
  - Platform protection domain.
  - Application protection domain.
  - An application protection domain is bound to a platform protection domain.
  - Each application’s group context is only bound to its application protection domain.

Creating Custom Protection Domain

- In the Java Card 3 platform RI, application protection domain is assigned to an application based on the certificate used to sign the application bundle.
- The application protection domain configured in lib/config.properties file contains:
  - Certificate
  - Set of permissions

Permission Puzzle Answer

- With only following permission granted in the application protection domain:
  - javacardx.io.ConnectorPermission "https://*/*", "connect,listen,accept,read,write"
- What will happen when build the connection?
  - A - No exception
  - B - AccessControlException
  - C - Other exception
  - D - Other

Permission Puzzle Lesson

- Permissions may be granted on a per-application basis through an application protection domain.

User Authorization Puzzle

- **Web Deployment Descriptor[web.xml]**

```
  <security-constraint>
          <url-pattern>/remote</url-pattern>
          <http-method>GET</http-method>
      <auth-constraint>
           <role-name>ru</role-name>
      </auth-constraint>
  </security-constraint>
```

- **Java Card Runtime Descriptor[Manifest.mf]**
  - User-Role-List: ru, ch
  - ch-Mapped-To-Auth-URI:sio:///standard/auth/holder/global/admin/pin
  - ru-Mapped-To-Auth-URI: sio:///standard/auth/user/session/Joe/pin
- **Java Card Platform Descriptor[javacard.xml]:** 'ch'

User Authorization Puzzle

- Joe belongs to the 'ru' role category
  - Is a remote user
- Joe has the correct user name and password
- Joe tries to access the 'remoteServlet' from a remote machine
- Joe:
  - A. Is prompted for user name and password
  - B. Is denied access because he is not an authorized user for this resource
  - C. Is denied access because he needs Card Holder Authorization to access the resource

User Classification

- The Card Holder
- The Other/Remote User
-

Determining Accessibility Requirements

- A web application
  - Card Holder Facing
  - Remote User Accessible

Card Holder Authorization Requirements for Access by User

Access From

		Locally Accessible Application	Remotely Accessible Application
Access To	Card Holder Facing Client	Not Required	Not Required
	Non Card Holder Facing Client	Rejected	Required

Note: Card Holder Authentication can only be done by a Card-Holder facing application!

Card Holder Authorization

```
javacard.xml:platform descriptor

<card-holder-authorization>
<role-name>ch</role-name>
</card-holder-authorization>
```

User Authorization Puzzle Answer

- Joe belongs to the 'ru' role category
  - Is a remote admin
- Joe has the correct user name and password
- Joe wants to access the 'remoteServlet' from a remote machine
- Joe:
  - A. Is prompted for user name and password
  - B. Is denied access because he is not an authorized user for this resource
  - C. Is denied access because he needs Card Holder Authorization to access the resource

User Authorization Puzzle Lesson

- Card Holder authorization, in relevant role, required, for remotely accessible applications
- Java Card platform deployment descriptor must include:
  - a `card-holder-authorization` element
  - one or more `role-name` sub-elements designating role names mapped to card-holder-users, see `card-holder-authorization`

User Authentication Puzzle

- A user, say 'admin', presents valid credentials to an application and can access the security constrained resource
  - Runtime descriptor maps this user to a global authenticator
- He closes the browser
- What will happen, when he tries to access the resource again:
  - A. He is prompted to enter user name and password
  - B. He is not prompted to enter user name and password and provided access to the resource
  - C. He is denied access

Authentication Schemes

- Authentication
    - Global
        - Applicable to Card Holder only
    - Session Scoped
        - Applicable to Card Holder
        - Applicable to other user
-

Authenticators

- Authentication Services: Authenticators
- Authenticator URIs
  - `sio:///standard/auth/holder/global/[<`*realm*`>/]<`*user*`>/<`*scheme*`>`
  - `sio:///standard/auth/holder/session/[<`*realm*`>/]<`*user*`>/<`*scheme*`>`
  - `sio:///standard/auth/user/session/[<`*realm*`>/]<`*user*`>/<`*scheme*`>`

  Scheme: PIN,Password,Biometric
- Java Card Deployment Descriptor

  -
    ```
    User-Role-List: ch
    Primary-Mapped-To-Auth-URI:
    sio:///standard/auth/user/global/admin/pin
    ```
-

User Authentication Puzzle Answer

- A user, say 'admin', presents valid credentials to an application and can access the security constrained resource
  - Runtime descriptor maps this user to a global authenticator
- He exits the browser accidently
- What will happen, when he tries to access the resource again:
  - A. He is prompted to enter user name and password
  - B. He is not prompted to enter user name and password and provided access to the resource
  - C. He is denied access

User Authentication Puzzle Lesson

- User credentials can be valid beyond a session
  - As in case of a user mapped to global authenticator

Lessons learned I

- Do not rely on persistence of servlets not configured as load-on-startup
- Do not use transient objects in transactions
- SecurityException will be thrown on the attempt to access object from not owing context
- Use of static fields in extension library can block the deletion of application using this library

Lessons learned II

- Web application can define the security requirements in its web application deployment descriptor and/or runtime descriptor.
- Certain set of permissions can be granted to an application through application protection domain
- Remotely accessible applications need card holder authorization for access
- User credentials can be valid beyond a session

What is next?

- Try Java Card 3.0.1 Platform
  - http://java.sun.com/javacard/
  - Demos in the Pavilion
- Use the recipes
- Avoid possible pitfalls
- Send us your Java Card Puzzlers

- The Most Important ...

Have fun with Java Card !!!

JavaOne℠

Thank You

Alexander Glasman,
Hema Kalsi, Thierry Violleau,
Lichun Zhan

Sun Microsystems, Inc.
www.sun.com