Lesson 07
JavaCard
Java Card

- Has CPU with limited processing command and low clock frequency operations
- An IC card—4 kB ROM
- A microprocessor card with 18 kB flash read only memory
JavaCard (Java for card)

- A micro-edition of Java for the cards
- A limited-memory sized edition for cards, labels, tokens, and similar devices which have limited memory as well as processing capacity
JavaCard 2.2.2

- Provides interoperability for cards and APIs for highly memory-efficient applications
- Has multiple communication interfaces for inter card-host contact/contactless (wireless) communication APIs
JavaCard 2.2.2

- ISO7816-based Extended length APDU support
- 20 maximum number of logical communication channels
- Provides standard communication with the host using latest SIM cards
javacard.security and javacard.crypto

- Supports digital-signature-based message recovery and advanced cryptography class libraries for HMAC-MD5, HMAC-SHA1, and SHA-256
Java Card framework (javacard.framework)

- Provides the library functions, Card interfaces, PIN (personal identification number), and ISO 7816 APIs for Card applet
- JCardSystem—a class in JavaCard, has a method `makeTransientArray()`
- The method creates a transient array and it persists till power is down
JavaCard Profile

- A set of limited class libraries
- SmartCard Profile—has a separate virtual machine called card VM
The card VM

• Different for different card OSes
JavaCard Executive

- Provides communication I/O streams between the JavaCard APIs and supports interoperability among the cards from different hardware and different card OSes
Card virtual machine (CardVM)

• Has an instruction set for a subset of Java language
• Installs applets and libraries into Java Card-based devices
• CardVM does not support weak reference as already mentioned for KVM
CardVM

- A virtual machine which has no char
- No double precision, or single precision
- No floating point mathematical operations support
- supports only Boolean, 8 bit Byte, BCD, 6 bit integer (short) (32 bit integer support optional)
- Limited exceptional handling
CardVM

- No object clones
- No String class libraries
- No automatic garbage collection (memory freeing)
- No native support using JNI (Java native interface) to use C/C++ application interface with the Java APIs
CardVM

- No SecurityManager class libraries
- No multi-threading
- No ThreadGroup
Card applets

- For application execution
- Java class libraries of the application
Card applets

- Java Card is a technology which supports a secure environment for smart cards and small-devices applets
- Multiple applets can be deployed on a single card and new ones can be added any time at the user end
card Applet

- Creates card-specific byte code on compilation
- Java applet has lifecycle starting from initiate, followed by start, stop, and destroy
Applet for communication

- Uses select method for selecting the process APDU whether it is a command APDU or response APDU
- Card applet differs from Java applet as it can reside permanently on card
- Objects created by card applet are persistent
- When applet is deselected the transient array disposes
Applet for communication

- Command APDU identifies a class for instruction, finds specific instruction from the class, uses two bytes for two parameters of the instruction, and specifies the length of optional data with the APDU.
- Response APDU has data (optional) and two bytes for status words.
JCRE (Java Card runtime environment)

- Interprets the card byte codes and implements them using Java Card virtual machine
- Does not support inter-communication between different card applets
- Provides runtime support to the services like selection and de-selection of applets
Summary

- JavaCard—A limited-memory sized edition for cards, labels, tokens, and similar devices which have limited memory as well as processing capacity
- javacard.crypto and javacard.security
- Card Profile
- Card VM
- Card Applet
End of Lesson 07
JavaCard