Security and Trusted Hardware Applications
Week #4 Tutorial

Pedro Antunes - up201507254

May 30, 2022

Instructor: Bernardo Portela

1

The four main memory types present in smart card solutions are:

- **RAM** (Random Access Memory) - It is an ephemeral (non-persistent) memory, which is essentially used to store temporary data used mainly for flow control of applications running on the Java Card. To be available it needs to have power. Whenever the power is turned off, all registers stored in RAM are freed. It can be accessed an unlimited number of times.
- **ROM** (Read-Only Memory) - It is a persistent memory, which can only be written once when java card was manufactured.Therefore, the information that resides in ROM cannot be modified. This memory stores the operating system code and boot data and doesn't need power to maintain this data.

  It can be accessed an unlimited number of times.
- **EEPROM** (Electrical erasable programmable read-only memory) - Assimilates with ROM, when it is a persistent memory that doesn't need power to maintain data. On the other hand, can accept up to 500,000 write cycles and retains the informations for 10 years. Her reading speed is as fast as RAM, but writing is 1000 times slower.
- **FLASH** - It is persistent mutable memory and it derives from EEPROM. However, it is more power efficient than its predecessor by updating only as a block. It is used to store programs, as well as EEPROM, or large chunks of data.

The main differences between ROM and EEPROM are related to writing data. ROM is too slow to write. Therefore, it is intended for data that will not be changed in the system. EEPROM allows persistent data to be written (as in ROM) but faster, so it is the memory used to store persistent data for Java Card applications, like storing applet data.

2

To maintain the information from multiple communications established by a card, persistent objects are used. These objects take longer to process because they ensure atomic instructions and because they are stored in EEPROM or FLASH memory. We must be concerned about persistent storage space so that it does not become full.

To optimize processing time we should use objects that are stored in RAM whenever possible. Therefore, we should use transient objects in this situations, which are the objects for storing information in RAM.

3

If the card is disconnected at the time the transient object is created and before the operation to add the new value to the pnt object starts, then the new point value stored in the transient object is lost and the operation will not perform successfully.

4

a) If the total value of valA + valB was 10, and we are constantly subtracting 1 from valA and adding 1 to valB, then to total value becames 9 the card was disconnected after "Remove 1 from valA" operation and before "Add 1 to valB" operation.

b) A operation atomicity means that there is a write attempt to a single persistent object field is guaranteed to either completed successfully, or else be restored to its original value before the operation starts if an error occurs during the update.

c) To prevent these failures we can use atomic operations or if we need more than 1 operations, we can use transactions. In this case we should use transactions since we have 2 operations that need such protection. It also possible to perform integrity checks before the card operations began.

5

a) The current full members of the GP can be found here. Numerous large companies are included in this association such as Mastercard, VISA, Apple or Cisco.

b) GP associaton try to create collaborative and open ecosystems in which all stakeholders can deliver digital services and devices, while providing greater end-to-end security, privacy and regulations. To perform this features, It aims to standardized technologies and certifications for trusted digital services and devices.

c) Certifications help raise the trustworthiness of real-world services or devices. Certifications are based on security standards that are based on the security definition of the respective global community. These certifications come to rest and bring better data protection for all entities in the market, both companies and customers.