Names: MIDN Ally Annick, USN

MIDN Kevin Nguyen, USN

Course: SY308 - Security Fundamental Principles

Assignment: Project 2: ATM Redesign Design Document

Reference: Project 1 Design Document

**PIN and Key Storage**

Our system stores the keys in the secure system bank and ATM files. However, balances are stored only in the secure bank file.

* ssBank.bin:
  + First line: AES encryption key
  + Following lines: user;pin;balance
* ssATM.bin:
  + First line: AES encryption key
  + Following lines: user;pin

**Cryptographic Schemes**

AES CTR encryption is used in all communications. This prevents anyone from eavesdropping on the router and intercepting commands. This also prevents someone from crafting commands and sending them to the bank’s socket as well. The reason we chose AES CTR is because it is a stream cipher; since the bank and ATM commands vary in length, using a stream cipher would simplify the encryption process and adhere to the security principle of Economy of Mechanism.

**Communication of Bank.py and ATM.py**

The messages are encrypted before being sent using AES CTR encryption. They travel over the wire (through router.py) encrypted, and are decrypted at the endpoint. Both bank.py and atm.py have the symmetric encryption key in their respective secure storage files.

**Card Structure**

The cards will contain only the user’s name. All PINs will be stored on the secure storage files. This card structure works in accordance with our program architecture of user verification taking place on bank.py with ATM.py acting only as a pipe through which the bank.py and user communicate. The minimal information stored on the cards increases the user’s security because all sensitive information (PINs, balances) is stored in secure storage. Further, all communication regarding this information is encrypted using AES encryption.

In order to use the atm, you must copy the card file over to inserted.card. This is equivalent to typing the name of the desired user into inserted.card.