Taha Mehdi
Pratik Patel
Chris Renus

Cryptography and Network Security I
CSCI-4971-01
Final Project

Protocol:

Backup Protection

All accounts are backed up for protection against power outage attacks. The protocol backs up all accounts within a 5 second window to an encrypted AES file on the bank.

The account_data.data file is checked upon the bank starting. If the file exists it will read the accounts from that file, otherwise the default accounts are initialized.

If time permitted this would have been better suited as a SQL database but due to resource limitations we took the file backup approach.

Packet Padding:

All packets are padded to 992 bytes to prevent adversaries obtaining information based upon packet length.

Packet Encryption

All input is combined with a hash to to detect tampering with packets. The hash is created using Sha-512. The packet is then encrypted with AES using a secret 128bit key.

Key Exchange

The initial connection/handshake is set up using RSA. The public keys for RSA are stored in a file corresponding to that machines id. The ATM encrypts its id using the banks public key and then creates a hash out of this ciphertext and the salt using sha-512. This is then sent along to the bank. The bank then calculates a hash of the ciphertext and the salt and compares to the attached hash. If they match, the bank decrypts the ciphertext using its private key and gets the atms id. The bank then generates a random AES key and encrypts it using the atms public key. Next the bank generates a checksum and sends it along with the ciphertext back to the ATM. The ATM will then calculate the checksum and if they match, the session is established and they have a secret key for AES to communicate with.

Synchronization Protection

Locks exist for each account to prevent synchronization errors.

Banking Error Protection

Integer datatype is used to hold balances. We protect against overflows by installing a bank limit for the amount of money that can exist per account.

Negative transfer/deposit commands are not allowed.

ATM Login Protection:

On account creation a card is generated for the particular account; this involves creation of a card hash. The card hash, the pin, and the appwide salt is used to generate an overall account hash for the account which is used to check for authentication. Accounts are allowed 3 login attempts before getting locked out.