Proposed Bank and ATM Protocol

Jason Parham, Matt O'Brian, Tyler Cassetta-Frey

November 21, 2012

Protocol Summary

The protocol proposed is a communication protocol designed for use between a bank and ATM with great security.to protect against various attacks. It was implemented using the Crypto++ library. From the ATM user's perspective, they are required to log in with a valid pin (which will be masked) and are automatically logged out after 3 minutes (180 seconds) of inactivity. In addition, they may only deposit, transfer, and withdraw $1000 per day. Finally, they may only have a maximum of $2,000,000,000 dollars in their account.

On the ATM and bank's side, hashing is done with 128-character hexadecimal SHA-512 while RSA is used for asymmetric encryption and AES-256 is used for symmetric encryption. Every nonce is 256-bit (32 characters). The ATM and bank both have handshakes. ATM handshake consists of "handshake", the new ATM nonce, the last bank nonce, random padding of 894 characters (1023-128-1), and the hash of the handshake. Finally, it is then encrypted using RSA. The bank handshake is done similarly, except that it contains the new bank nonce and the last ATM nonce.

ATM messages consist of the command, the username, card number, and pin all hashed, the dollar amount (if the command requires one), the user receiving the money (hashed, also only included if money is being transferred), the new ATM nonce, random padding, and either the last bank nonce or a handshake if the user is logging in.. The bank's response message consists of the command, appropriate message, the last ATM nonce, the new bank nonce and random padding. The message returned will be whether or not the action was successful (for login, logout, and transfer), the current balance (for balance), or the amount withdrawn (for withdraw). The message is then hashed and encrypted with AES. The messages will always be sent as 1408 characters after encryption.

A quick over view is shown below:

- After connecting to the bank, when the user logs in, the bank establishes session keys to be used and encrypts them using RSA.
- The ATM receives the handshake and checks to see if the hashes match.
- If the hashes match, the ATM decrypts the packet and retrieves the session keys.

    - Otherwise, it prints an error message.

- After establishing the handshake, the bank carries on with normal functionality.
- The ATM prompts the user for a command and verifies it's a valid command.
- Before sending a message, the ATM and bank both check to make sure the packet is 1408 characters before decrypting and performing the command.
- For each command, the bank and ATM will confirm that the nonce sent to it is correct.
- The bank confirms that the commands and hashes sent are both valid and appropriately used (exactly 2 name hashes are sent for transfer and exactly 1 for login commands)..
- If the user logs out or the session expires, the bank and ATM discard the session keys.