Vulnerability Report

Cryptography and Network Security I

CSCI-4971-01

Taha Mehdi **Pratik Patel** **Chris Renus**

Power Outage Attack

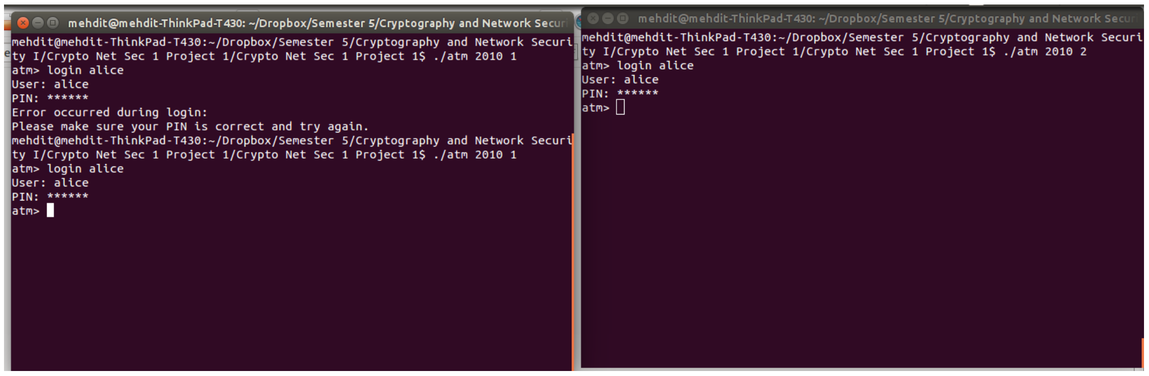
The other team stores each account in a vector that resides in a "Bank" class. Due to these accounts residing in memory, when the bank is closed all accounts are wiped. Therefore, we can in turn create a power outage attack against the bank (EMP attack) and force the computer running the bank server to close. Now all accounts will be deleted and since there is no backup of accounts, the bank cannot know what the accounts balances were.

Concurrency Issues

The accounts do not have a lock to prevent multiple ATMs to write to balance at the same time. If a user A is transferring money to user B, and at the same time user C is transferring money to user B there can be race conditions. If user B initially has $1000, both A and C can read that value and transfer $500. Therefore, instead of user B ending up with $2000, they will only have $1500. Another possible condition is user A login from 2 ATMs and has a balance of $100. It is possible to withdraw $100 from each ATM and actually withdraw $200 in total.

Multiple ATM Sessions

The other team allows the same user to login at multiple ATMs. This is invalid since there should only be one ATM card per user and so allows for copies of cards to be created.



```
mehdit@mehdit-ThinkPad-T430:~/Dropbox/Semester 5/Cryptography and Network Securi
ty I/Crypto Net Sec 1 Project 1/Crypto Net Sec 1 Project 1$ ./atm 2010 1
atm> login alice
User: alice
PIN: ******
Error occurred during login:
Please make sure your PIN is correct and try again.
mehdit@mehdit-ThinkPad-T430:~/Dropbox/Semester 5/Cryptography and Network Securi
ty I/Crypto Net Sec 1 Project 1/Crypto Net Sec 1 Project 1$ ./atm 2010 1
atm> login alice
User: alice
PIN: ******
atm>
```

```
mehdit@mehdit-ThinkPad-T430:~/Dropbox/Semester 5/Cryptography and Network Securi
ty I/Crypto Net Sec 1 Project 1/Crypto Net Sec 1 Project 1$ ./atm 2010 2
atm> login alice
User: alice
PIN: ******
atm>
```

Denial of Service (DoS) Attack

In this protocol there can only be 50 ATMs running at the same time. Since there is no stopping a user from logging in from multiple ATMs, we can create a DoS attack by logging in to every ATM. Since there is no timeout feature to logout a user, once there are 50 ATMs occupied, no other user can use the bank.

Bank Commands

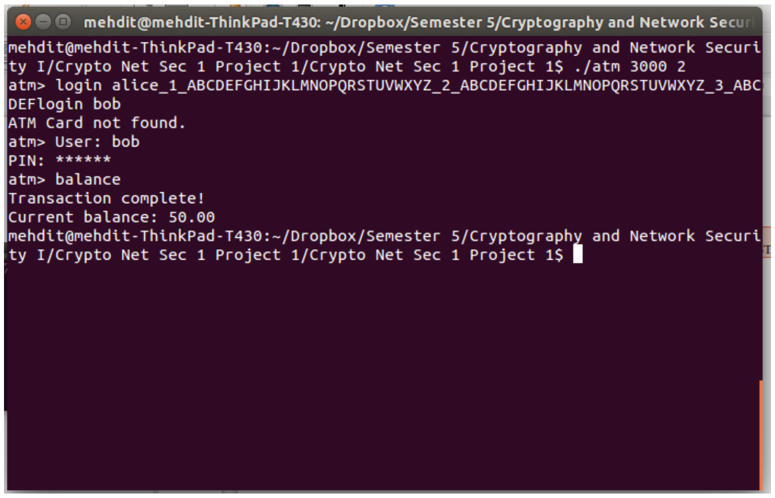
Through the bank terminal by using the balance command, it tells whether the account is valid or not. Through this, the team is able to gain information on all possible users within the bank.

Bank Usage Issues

The team has found many features that will detriment usage for the end user. For example, every time a command is entered at an ATM, the user is then logged out. This is poor user experience and does not emulate a real-world ATM. There exists a deposit, transfer, and withdraw limit for each individual account. These limits include 3 transfer attempts, $1,000 total withdraw limit, and $1,000,000,000 total deposit limit. This is an issue because you are able to deposit more than you can withdraw therefore allowing the bank to keep your money.

Multiple Command Input

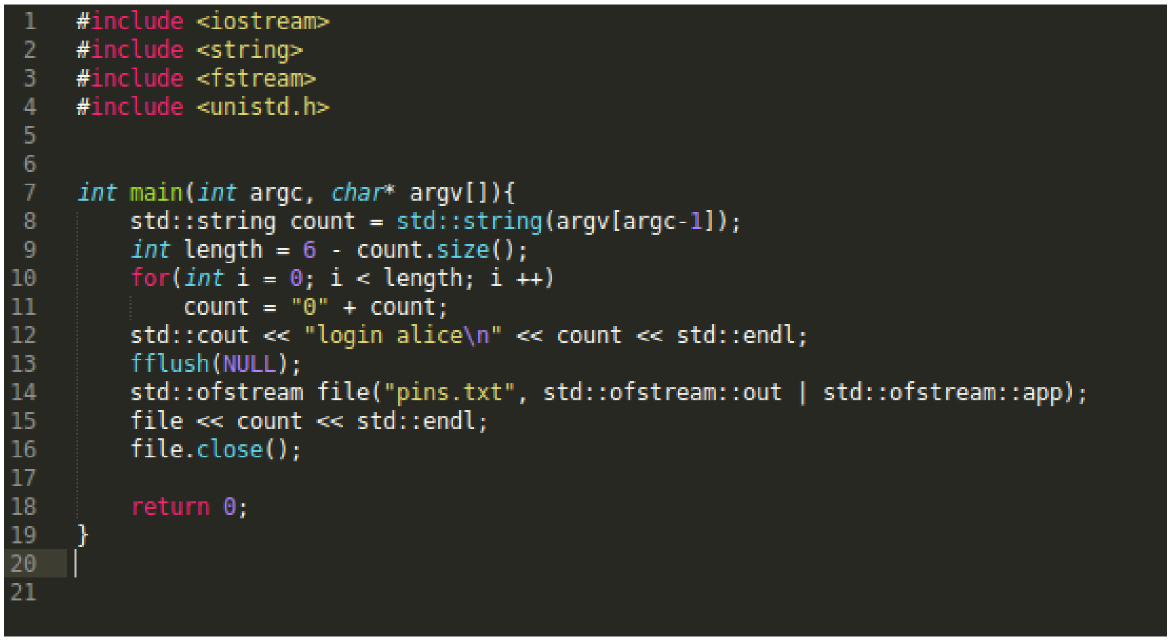
The input buffer for the command is of length 80. Because of the looping structure of how the code is read, a command such as login alice_1_ABCDEFGHIJKLMNOPQRSTUVWXYZ_2_ABCDEFGHIJKLMNOPQRSTUVWXYZ_3_ABCDEFlogin bob (i.e. a valid input command, followed by a string such that the length of the command plus the length of the string plus 1 for the space is equal to 78) yields for the possibility to execute simultaneous commands.



```
mehdit@mehdit-ThinkPad-T430: ~/Dropbox/Semester 5/Cryptography and Network Secur
mehdit@mehdit-ThinkPad-T430:~/Dropbox/Semester 5/Cryptography and Network Securi
ty I/Crypto Net Sec 1 Project 1/Crypto Net Sec 1 Project 1$ ./atm 3000 2
atm> login alice_1_ABCDEFGHIJKLMNOPQRSTUVWXYZ_2_ABCDEFGHIJKLMNOPQRSTUVWXYZ_3_ABC
DEFlogin bob
ATM Card not found.
atm> User: bob
PIN: ******
atm> balance
Transaction complete!
Current balance: 50.00
mehdit@mehdit-ThinkPad-T430:~/Dropbox/Semester 5/Cryptography and Network Securi
ty I/Crypto Net Sec 1 Project 1/Crypto Net Sec 1 Project 1$
```

Infinite Login Attempts

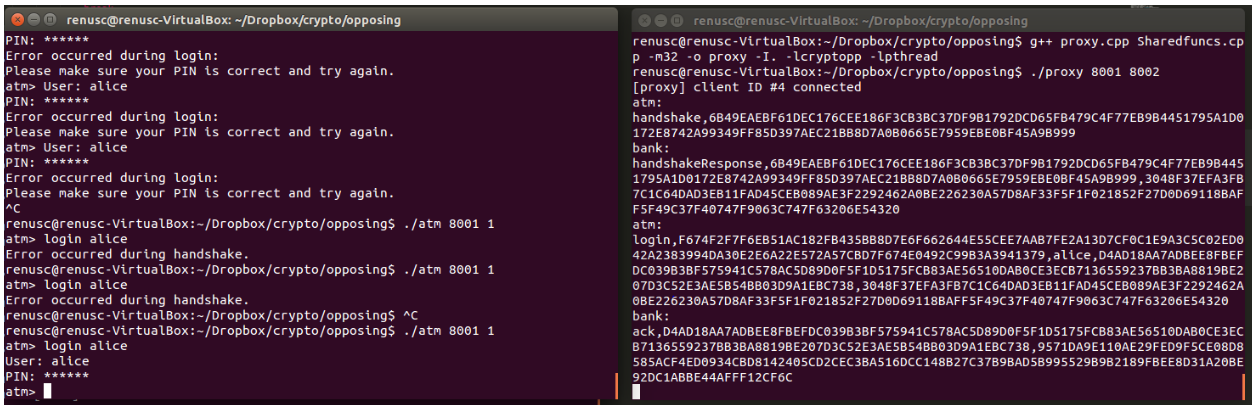
The other team has not taken the precautions to limit the number of times a user can attempt to login to an account. Therefore we are able to crack these pins by trying various number of pins (000000 - 999999). The team wrote code (seen below) to crack the pins; the approximate time to attempt 5000 pins was 10 minutes, so all possible pins would be recovered in around 33 hours using a laptop.



```cpp
#include <iostream>
#include <string>
#include <fstream>
#include <unistd.h>


int main(int argc, char* argv[]){
    std::string count = std::string(argv[argc-1]);
    int length = 6 - count.size();
    for(int i = 0; i < length; i ++)
        count = "0" + count;
    std::cout << "login alice\n" << count << std::endl;
    fflush(NULL);
    std::ofstream file("pins.txt", std::ofstream::out | std::ofstream::app);
    file << count << std::endl;
    file.close();

    return 0;
}

```

AES Keys

The AES keys are stored in a file called keys. Upon creation of the bank, all keys are generated and stored within this file and stored onto the ATM. This means that through purchasing an ATM, the keys can be extracted. The image below on the right shows the decrypted packet. All packets can be seen in plaintext along with the nonce.



```
PIN: ******
Error occurred during login:
Please make sure your PIN is correct and try again.
atm> User: alice
PIN: ******
Error occurred during login:
Please make sure your PIN is correct and try again.
atm> User: alice
PIN: ******
Error occurred during login:
Please make sure your PIN is correct and try again.
^C
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ ./atm 8001 1
atm> login alice
Error occurred during handshake.
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ ./atm 8001 1
atm> login alice
Error occurred during handshake.
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ ^C
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ ./atm 8001 1
atm> login alice
User: alice
PIN: ******
atm> 
```

```
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ g++ proxy.cpp Sharedfuncs.cp
p -m32 -o proxy -I. -lcryptopp -lpthread
renusc@renusc-VirtualBox:~/Dropbox/crypto/opposing$ ./proxy 8001 8002
[proxy] client ID #4 connected
atm:
handshake,6B49EAEBF61DEC176CEE186F3CB3BC37DF9B1792DCD65FB479C4F77EB9B4451795A1D0
172E8742A99349FF85D397AEC21BB8D7A0B0665E7959EBE0BF45A9B999
bank:
handshakeResponse,6B49EAEBF61DEC176CEE186F3CB3BC37DF9B1792DCD65FB479C4F77EB9B445
1795A1D0172E8742A99349FF85D397AEC21BB8D7A0B0665E7959EBE0BF45A9B999,3048F37EFA3FB
7C1C64DAD3EB11FAD45CEB089AE3F2292462A0BE226230A57D8AF33F5F1F021852F27D0D69118BAF
F5F49C37F40747F9063C747F63206E54320
atm:
login,F674F2F7F6EB51AC182FB435BB8D7E6F662644E55CEE7AAB7FE2A13D7CF0C1E9A3C5C02ED0
42A2383994DA30E2E6A22E572A57CBD7F674E0492C99B3A3941379,alice,D4AD18AA7ADBEE8FBEF
DC039B3BF575941C578AC5D89D0F5F1D5175FCB83AE56510DAB0CE3ECB7136559237BB3BA8819BE2
07D3C52E3AE5B54BB03D9A1EBC738,3048F37EFA3FB7C1C64DAD3EB11FAD45CEB089AE3F2292462A
0BE226230A57D8AF33F5F1F021852F27D0D69118BAFF5F49C37F40747F9063C747F63206E54320
bank:
ack,D4AD18AA7ADBEE8FBEFDC039B3BF575941C578AC5D89D0F5F1D5175FCB83AE56510DAB0CE3EC
B7136559237BB3BA8819BE207D3C52E3AE5B54BB03D9A1EBC738,9571DA9E110AE29FED9F5CE08D8
585ACF4ED0934CBD8142405CD2CEC3BA516DCC148B27C37B9BAD5B995529B9B2189FBEE8D31A20BE
92DC1ABBE44AFFF12CF6C
```

Nonces

The nonces do not serve much purpose. They are not a hash of the plaintext and so there is no checking of tampering. The nonces are just transferred to the other side without being a hash of anything and can be copied and used to act as the other side. The nonces are not dependent upon anything during the initial handshake and so there is no authentication or validation so an adversary could impersonate the bank, create a nonce, and the ATM would have no idea. Therefore, with the AES cracked, this would allow for a user on the ATM to login to any account, with any pin, and withdraw all of the money from the ATM without ever contacting the bank.