Michael Garrett
Pao Fang
Joubin Jabarri

CSC 250 Programming Assignment
Multi-Client/Server Electronic Voting System

I. Design Approach and Justification

a. Our approach to the design of our secure voting system places emphasis on confidentiality (preventing the disclosure of information to unauthorized individuals), integrity (maintaining and assuring the accuracy and consistency of data over its transmission between client and server) and authenticity (evidence that the message data is genuine and was sent by someone possessing the proper). The use of confidentiality, integrity and authenticity is known as CIA in the information security community. To meet the confidentiality requirement we used AES and RSA encryption/decryption to communicate from each client to the server. To meet the authenticity requirement we used hash functions to protect sensitive information such as the voter identification (VID). We envisioned the use of this system would require the acquisition of a VID for every registered voter from an offline system such as the DMV. This provided confidentiality for the voter. We used TCP to ensure reliable transmission. We used a hashed VID to maintain confidentiality of the voter's choices within the database. The RSA key pair is generated offline and the public key is embedded in the client code so that the client can send the VID hash to authenticate and establish a connection. In the real world application of this system we would use a certificate authority to verify the authenticity of the public key.

b. Client To Server
   i. $E_{pubServer}[sha256(vid),\ sha256(R1)] = k \text{ where } R1\ \varepsilon\ \{Randomly\ generated\ String\}$

c. Server To Client
   i. $[sha256(R2)] \text{ where } R2\ \varepsilon \{Randomly\ Generated\ String\}$

d. At this point, both client and server have three pieces of information in common
   i. clients sha256(vid) - Sent RSA encrypted
   ii. R1 - Sent RSA encrypted
   iii. R2 - Sent in plaintext

e. An external listener Eve, can have access to one of the three pieces of the information. R1 and R2 will generate a sha256 string which is to be used as a shared key.

f. Given half of a string that generates $sha256(R1 \mid\mid R2)$ it is virtually impossible to find the reverse of this. Sha by design is a one way function and we can assume with a high probability than an attacker will not be able to reverse the sha.

II. Advantages and Disadvantages

a. The advantage to our system is the adherence to the CIA standard. We went to great measure to ensure that "Eve," if listening to our transmission to the server, is not able to understand what is transmitted and is also not able to manipulate data so that the voters choice is incorrect or void.

b. The disadvantages to our system are that we did not include logging so that we could keep track of who was making changes to the system and when. We also didn't include separation of duties in our design. This would prevent the opportunity of a single user to make a change to the outcome of the election. In order for some malicious attempt to occur collusion would have to take place if two or more persons were involved.

III. List of Files (source code and executable)

a. README: contains build information
b. ClientStart.java
c. Login.java
d. VotingBallot.java
e. Connection.java
f. SizeDocumentFilter.java
g. ChainedDocumentFilter.java
h. VSCrypt.java

IV. Document Ownership

a. Garrett: VSCrypt.java, VS_docs
b. Jabarri: DB_handler.java, DB_connect.java, VotingSystem.java, EncrytDB, Server.java
c. Fang: ClientStart.java, ChainedDocumentFilter.java, Login.java, SizeDocumentFilter.java, VotingBallot.java, Connection.java

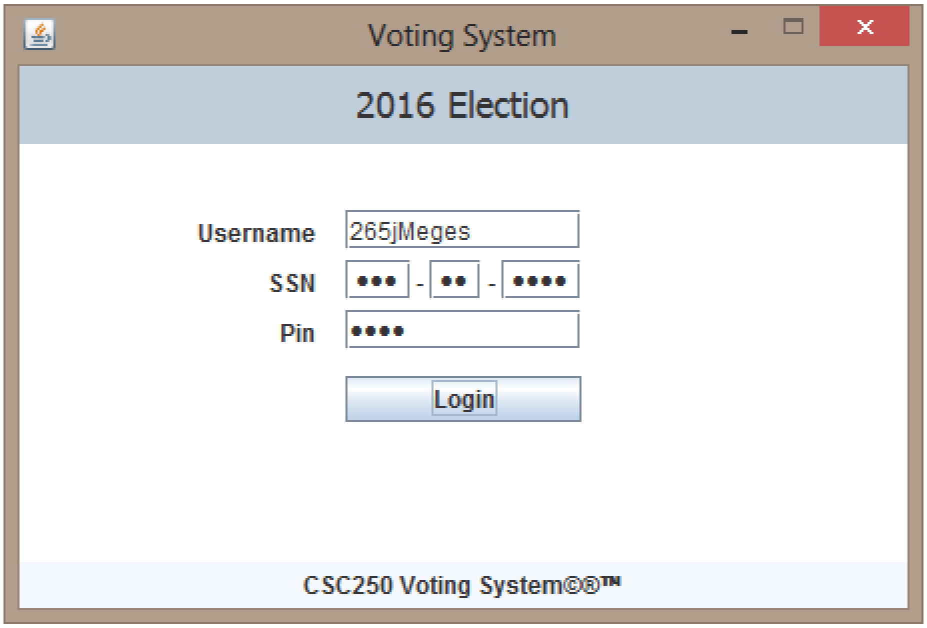
V. Challenges and Lessons Learned

a. Our first challenge dealt with how we handled the passing of encrypted/decrypted messages. Initially we were going to use RSA to establish an asymmetric cryptographic connection using the public key of the server to encrypt the initial contact to the server. After the client was authenticated we were going to establish a symmetric cryptographic connection using AES and an established session key. Our final design included this same idea however, each client was originally going to have its own thread. This proved difficult since each thread was terminating causing the state of the client connection to be lost. To ensure the server knew it was talking to an authenticated client and the state of the client could be maintained, the hashed VID was placed in the header of the JSON. This way the client could be identified upon subsequent communications.

b. Given more time, we would definitely add more security to the system. After learning about logging and and separation of duties, we feel that these security concepts belong to a secure voting system.

c. In our initial design we also decided to use different languages for different aspects of the system. Although a great learning experience, this proved to be rather troublesome. Pao wanted to use Java for the front end and Mike wanted to use Python for the client/server connection and the encryption/decryption of all communications. Joubin also wanted to do Python to implement the backend and interface with the database. The problem first arose when we began testing our system. The client would pass login and password to the connection class that would establish a TCP connection with the server and use the server's public key to encrypt the communication. The problem with encrypting in Java and then decrypting in Python is that Java uses PKCS (public key cryptography standard) #1 while Python uses PKCS #8 standard. The padding scheme of both standards are different and there are no solutions that are readily available to make appropriate conversions. This discrepancy made it impossible to maintain the integrity of the data. Our solution was to redo the entire Python portion into Java. Although time consuming and also problematic, this proved to be the better choice.

Login Window



Voting System

2016 Election

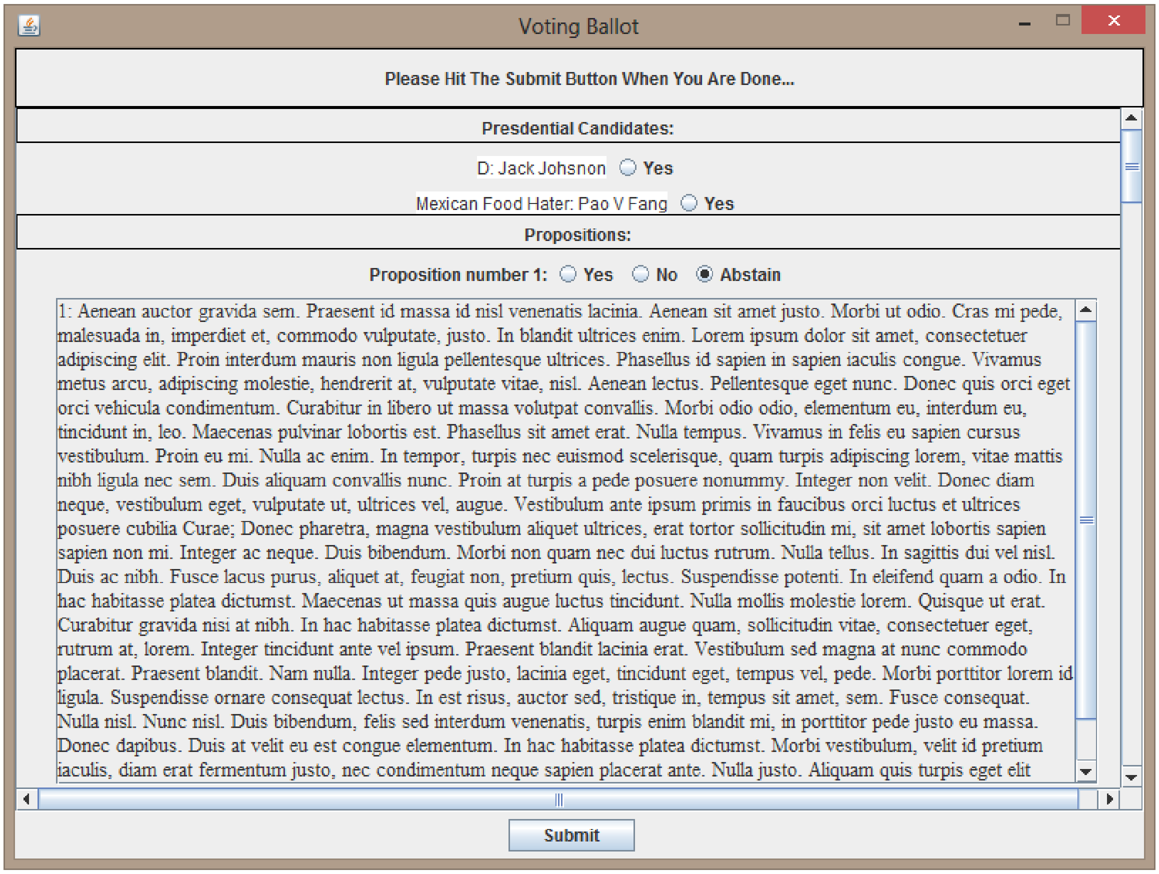
Username 265jMeges

SSN ●●● - ●● - ●●●●

Pin ●●●●

CSC250 Voting System©®™

Ballot and Presidential Candidates Received



Please Hit The Submit Button When You Are Done...

Presdential Candidates:

D: Jack Johsnon ○ Yes

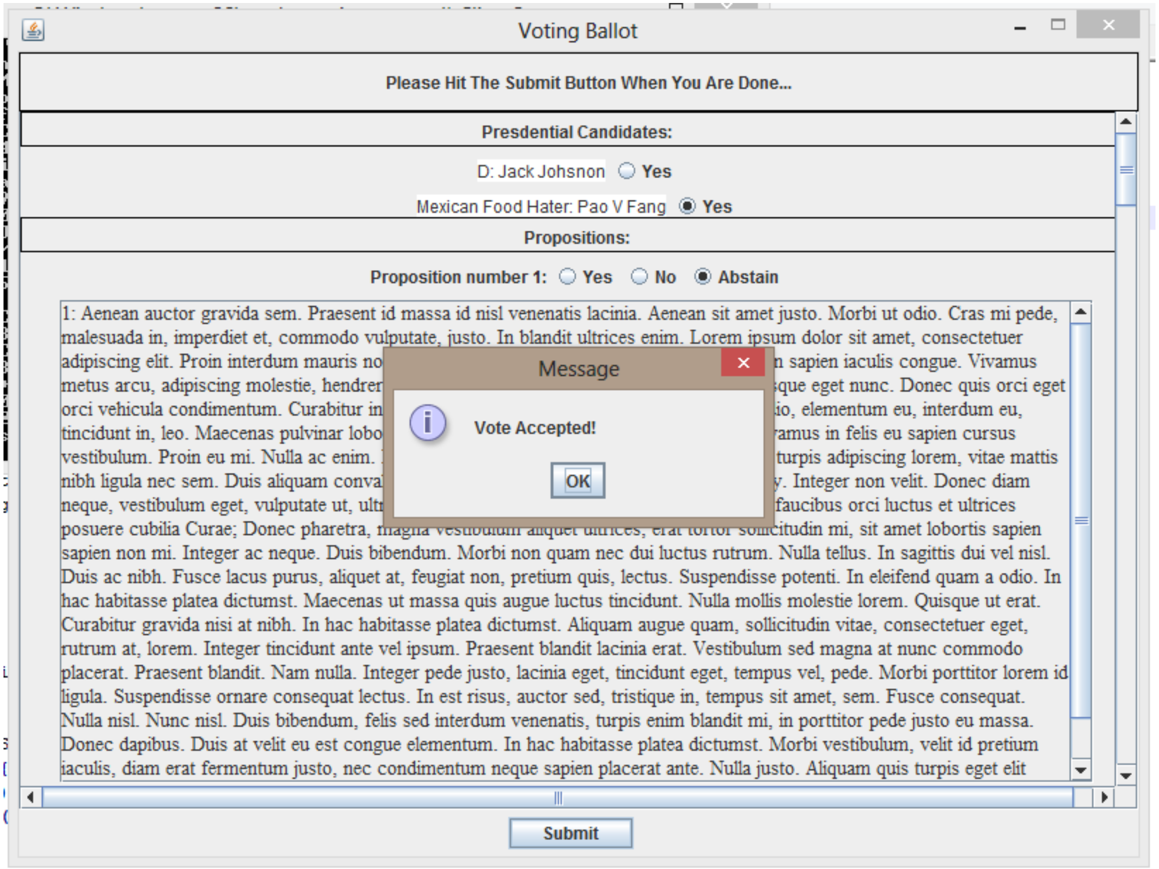
Mexican Food Hater: Pao V Fang ○ Yes

Propositions:

Proposition number 1: ○ Yes ○ No ● Abstain

1: Aenean auctor gravida sem. Praesent id massa id nisl venenatis lacinia. Aenean sit amet justo. Morbi ut odio. Cras mi pede, malesuada in, imperdiet et, commodo vulputate, justo. In blandit ultrices enim. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Proin interdum mauris non ligula pellentesque ultrices. Phasellus id sapien in sapien iaculis congue. Vivamus metus arcu, adipiscing molestie, hendrerit at, vulputate vitae, nisl. Aenean lectus. Pellentesque eget nunc. Donec quis orci eget orci vehicula condimentum. Curabitur in libero ut massa volutpat convallis. Morbi odio odio, elementum eu, interdum eu, tincidunt in, leo. Maecenas pulvinar lobortis est. Phasellus sit amet erat. Nulla tempus. Vivamus in felis eu sapien cursus vestibulum. Proin eu mi. Nulla ac enim. In tempor, turpis nec euismod scelerisque, quam turpis adipiscing lorem, vitae mattis nibh ligula nec sem. Duis aliquam convallis nunc. Proin at turpis a pede posuere nonummy. Integer non velit. Donec diam neque, vestibulum eget, vulputate ut, ultrices vel, augue. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Donec pharetra, magna vestibulum aliquet ultrices, erat tortor sollicitudin mi, sit amet lobortis sapien sapien non mi. Integer ac neque. Duis bibendum. Morbi non quam nec dui luctus rutrum. Nulla tellus. In sagittis dui vel nisl. Duis ac nibh. Fusce lacus purus, aliquet at, feugiat non, pretium quis, lectus. Suspendisse potenti. In eleifend quam a odio. In hac habitasse platea dictumst. Maecenas ut massa quis augue luctus tincidunt. Nulla mollis molestie lorem. Quisque ut erat. Curabitur gravida nisi at nibh. In hac habitasse platea dictumst. Aliquam augue quam, sollicitudin vitae, consectetuer eget, rutrum at, lorem. Integer tincidunt ante vel ipsum. Praesent blandit lacinia erat. Vestibulum sed magna at nunc commodo placerat. Praesent blandit. Nam nulla. Integer pede justo, lacinia eget, tincidunt eget, tempus vel, pede. Morbi porttitor lorem id ligula. Suspendisse ornare consequat lectus. In est risus, auctor sed, tristique in, tempus sit amet, sem. Fusce consequat. Nulla nisl. Nunc nisl. Duis bibendum, felis sed interdum venenatis, turpis enim blandit mi, in porttitor pede justo eu massa. Donec dapibus. Duis at velit eu est congue elementum. In hac habitasse platea dictumst. Morbi vestibulum, velit id pretium iaculis, diam erat fermentum justo, nec condimentum neque sapien placerat ante. Nulla justo. Aliquam quis turpis eget elit

Secure Voting Succe



Please Hit The Submit Button When You Are Done...

Presdential Candidates:

D: Jack Johsnon ○ Yes

Mexican Food Hater: Pao V Fang ● Yes

Propositions:

Proposition number 1: ○ Yes ○ No ● Abstain

1: Aenean auctor gravida sem. Praesent id massa id nisl venenatis lacinia. Aenean sit amet justo. Morbi ut odio. Cras mi pede,
malesuada in, imperdiet et, commodo vulputate, justo. In blandit ultrices enim. Lorem ipsum dolor sit amet, consectetuer
adipiscing elit. Proin interdum mauris no n sapien iaculis congue. Vivamus
metus arcu, adipiscing molestie, hendrer sque eget nunc. Donec quis orci eget
orci vehicula condimentum. Curabitur in io, elementum eu, interdum eu,
tincidunt in, leo. Maecenas pulvinar lobo ramus in felis eu sapien cursus
vestibulum. Proin eu mi. Nulla ac enim. turpis adipiscing lorem, vitae mattis
nibh ligula nec sem. Duis aliquam conva y. Integer non velit. Donec diam
neque, vestibulum eget, vulputate ut, ultr faucibus orci luctus et ultrices
posuere cubilia Curae; Donec pharetra, citudin mi, sit amet lobortis sapien
sapien non mi. Integer ac neque. Duis bibendum. Morbi non quam nec dui luctus rutrum. Nulla tellus. In sagittis dui vel nisl.
Duis ac nibh. Fusce lacus purus, aliquet at, feugiat non, pretium quis, lectus. Suspendisse potenti. In eleifend quam a odio. In
hac habitasse platea dictumst. Maecenas ut massa quis augue luctus tincidunt. Nulla mollis molestie lorem. Quisque ut erat.
Curabitur gravida nisi at nibh. In hac habitasse platea dictumst. Aliquam augue quam, sollicitudin vitae, consectetuer eget,
rutrum at, lorem. Integer tincidunt ante vel ipsum. Praesent blandit lacinia erat. Vestibulum sed magna at nunc commodo
placerat. Praesent blandit. Nam nulla. Integer pede justo, lacinia eget, tincidunt eget, tempus vel, pede. Morbi porttitor lorem id
ligula. Suspendisse ornare consequat lectus. In est risus, auctor sed, tristique in, tempus sit amet, sem. Fusce consequat.
Nulla nisl. Nunc nisl. Duis bibendum, felis sed interdum venenatis, turpis enim blandit mi, in porttitor pede justo eu massa.
Donec dapibus. Duis at velit eu est congue elementum. In hac habitasse platea dictumst. Morbi vestibulum, velit id pretium
iaculis, diam erat fermentum justo, nec condimentum neque sapien placerat ante. Nulla justo. Aliquam quis turpis eget elit

Vote Accepted!