Password Storage and Retrieval

Nitin K N[1] Sharath S Chellappa[2] Chetan Purohit[3]
Madhusudan Thyagarajan[4]

[1]USN-1PI13EC064 Electronics and Communication Department
PES Institute of Technology

[2]USN-1PI13EC092 Electronics and Communication Department
PES Institute of Technology

[3]USN-1PI13EC025 Electronics and Communication Department
PES Institute of Technology

[4]Professor Electronics and Communication Department
PES Institute of Technology

Phase 1, 9nd February 2017

Outline

Problem Statement

To design a bank system which ensures that compromise of any one server storing the password, never gives away the entire password of the user.

Objective

- The objective is to develop an app for a banking system where the user enters his password which is never completely stored anywhere.
- The Bank server splits the hashed password given to it into different pieces and stores these in geographically different locations.
- Nowhere does the Bank server or the Servers storing the pieces of password get to know what the complete password is. Hence compromise of the servers would never give away the users password as it is.
- The adversary would require multiple points of attacks in order to break the password.

Deliverables

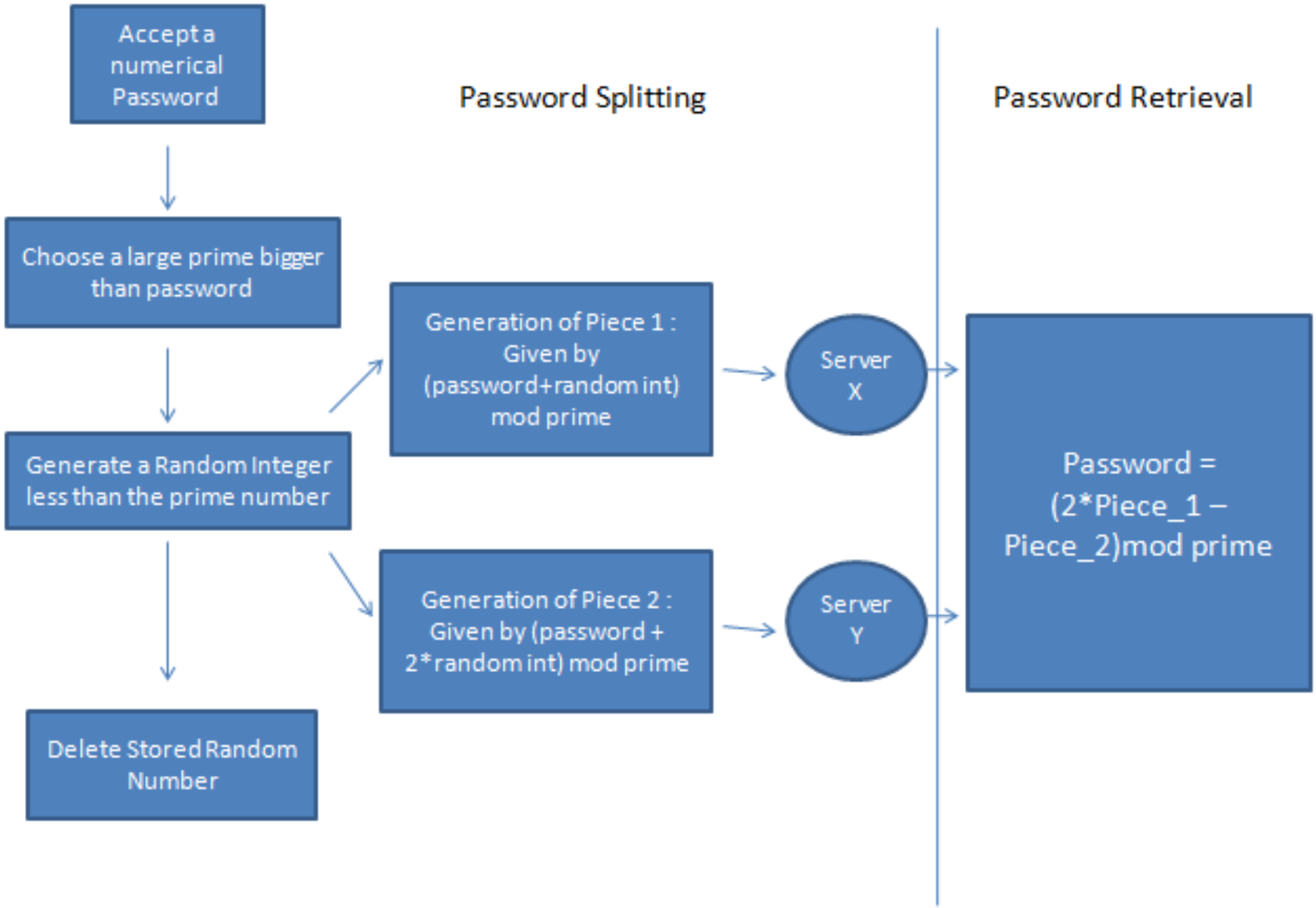
- User end Application
  - The end user interface of the application. This is what is displayed to the user.
  - Handling authentication of the user by the server.
- Algorithms
  - Implementation of splitting of password and recovery.[2]
  - Introducing a system which makes the application device specific. Generation of public and private keys, assymetrical encryption, hashing passwords.
- Inter Machine Communication
  - Secure Communication between the Device-specific Application and the Main Server.
  - Secure Communication between the Main Server and the Servers containing pieces of the password sent

Timeline

- Feasibility Report - Literature survey, architecture of System.
- Phase 1 - Communication between bank and split servers, Basic layout of the app, partial implementation of splitting of password.[2]
- Phase 2 - Communication between app and bank server, development of login page of the app, issue of keys and securing communication along with hashing.
- Phase 3 - Optimisation and end case testing of communication, development of sign up page, generation of location pass and making app device specific.
- Phase 4 - Integration of application with the servers.
- Final Presentation - Validation of results by simulation.

Password Splitting Implementation

How to share a secret, Shamir



Architecture

Password Retrieval

User clicks on the button to request access to his account

$E_{skb}\{E_{pku}\{\text{Login id}\}\}$

OTP

OTP

The Bank server correlates OTP with the login id. This correlation expires in a finite time.

The Bank Server decrypts the packet to get the login id and OTP, gets the location of the servers having pieces from the Location Pass and sends the login Id to each of the servers after checking if the OTP matches.

OTP + Password

$E_{skb}\{E_{pku}\{\text{OTP+login ID + Hash(User Password+OTP) + location pass}\}\}$

Hash(Login id) to each server

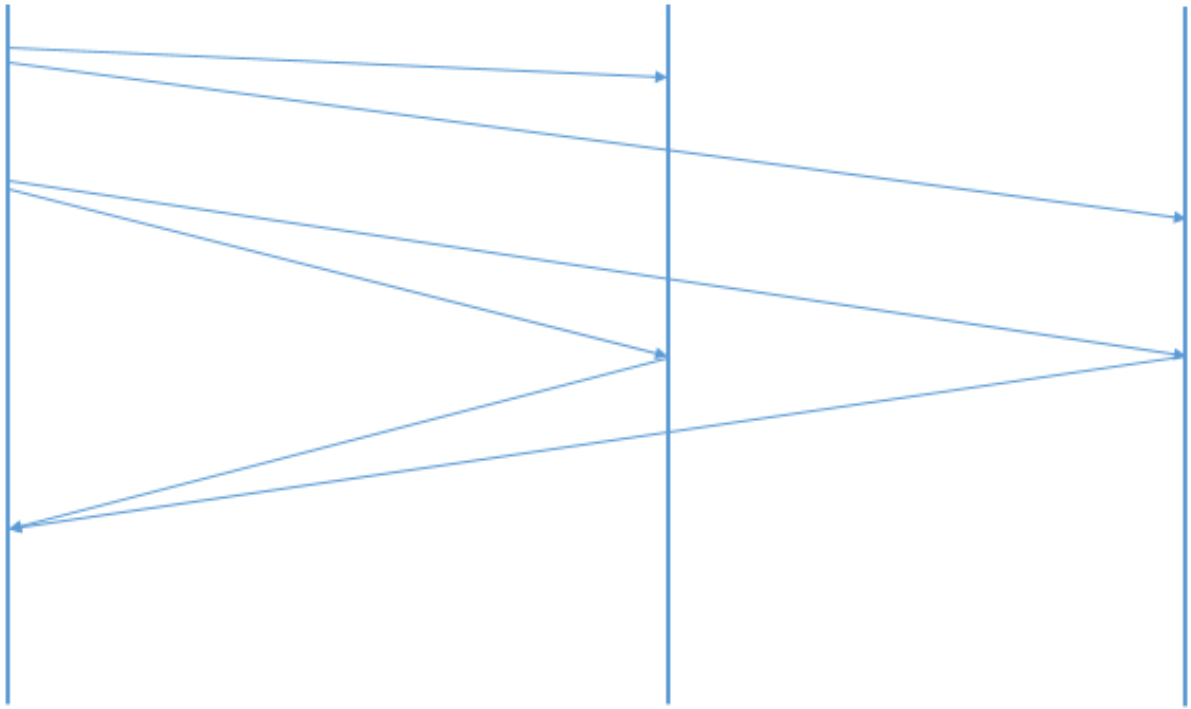
The user gets to access his account over a secure connection.

Returns Port number to set up connection with if there is a match

Each piece is sent to Bank Server

Implemented System

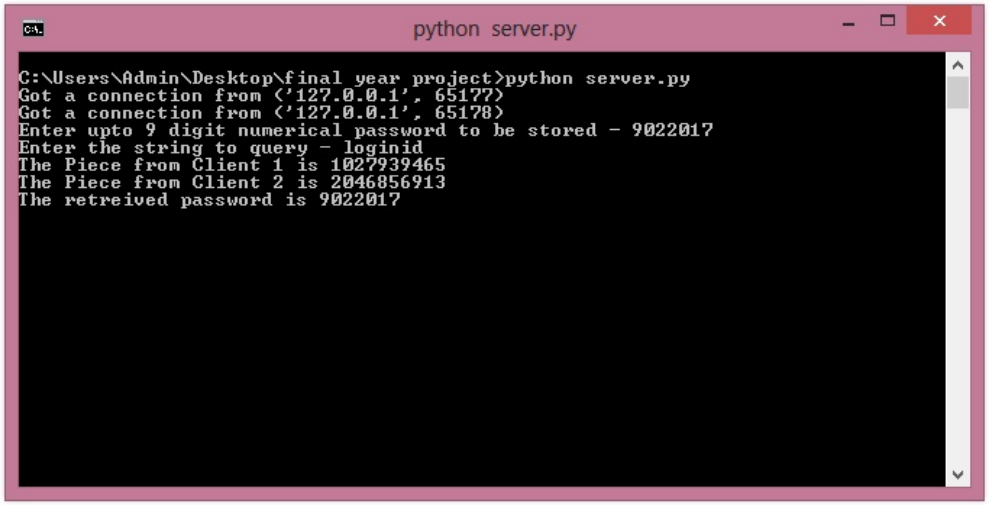
Phase 1

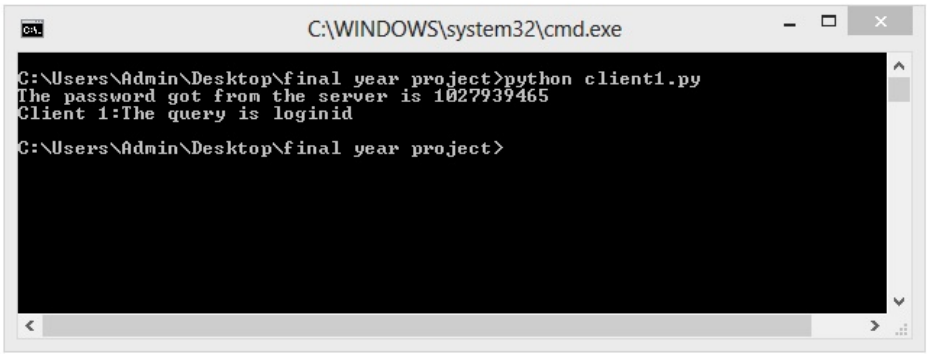


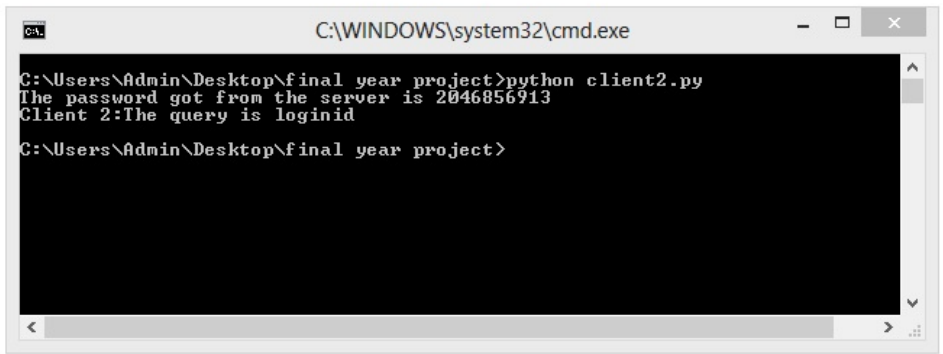
The password is entered into the bank server and split into 2 pieces by using the algorithm authored by Shamir. Each piece is sent to each split server, as a (key,piece) pair.

The bank server then sends a query to each of the split servers. The split servers reply with the corresponding piece for the corresponding key queried.

Current System Implementation







Timeline

- Feasibility Report - Literature survey, architecture of System.
- Phase 1 - Communication between bank and split servers, Basic layout of the app, partial implementation of splitting of password.[2]
- Phase 2 - Communication between app and bank server, development of login page of the app, issue of keys and securing communication along with hashing.
- Phase 3 - Optimisation and end case testing of communication, development of sign up page, generation of location pass and making app device specific.
- Phase 4 - Integration of application with the servers.
- Final Presentation - Validation of results by simulation.