Virtual One Time Password in Two-Factor Authentication

By Darren Yeh and Jack Conway Advisor Dr. Jing-Chiou Liou

Abstract

- Authentication is a process to determine whether or not if someone is actually who he/she declares to be.
- The most common and popular method of authentication is username/password, but it is also proven to be a very weak authentication technique.
- One time password (OTP) is a good way to enhance security by adding another factor to further verify user's identity. Having a virtual OTP will greatly increase security and reduce the chance of getting compromise.

Introduction

- In today's society, the Information Technology (IT) and internet have played a significant role among people's daily life.
- Not only does people share information through internet, but also transactions and services can be done online at anywhere and anytime.
- With all the conveniences that IT have brought, also come with a cost, security.

Background

- Authentication process generally require some factors for verification of user's identity.
- Authentication factor is a piece of information that is supplied by the user or of the user. Typically using one of the three method:
  - something the user knows (e.g. username/ password)
  - something the user has (e.g. token)
  - something of the user (e.g. fingerprint)

Single Factor Authentication

- This method of authentication relies only on one factor. The most common method of this is username/ password. Although it is proven to be a weak authentication technique, it is still widely used all over the world.
- Even with a strong password, phishing, spoofing attacks and key logger can trick the user into supplying the password.
- In addition, people usually do not charge their passwords frequently.

Two Factor Authentication

- Security tokens, also known as OTP token, have an LCD screen that displays set of number. The numbers will be randomly generated and act as the second factor.
- The token is based on two types of algorithms: time synchronized and event-based.
- Time synchronized will generated a set of number in a fixed amount of time. While the event-based will be triggered by user action such as pressing a button on the token.

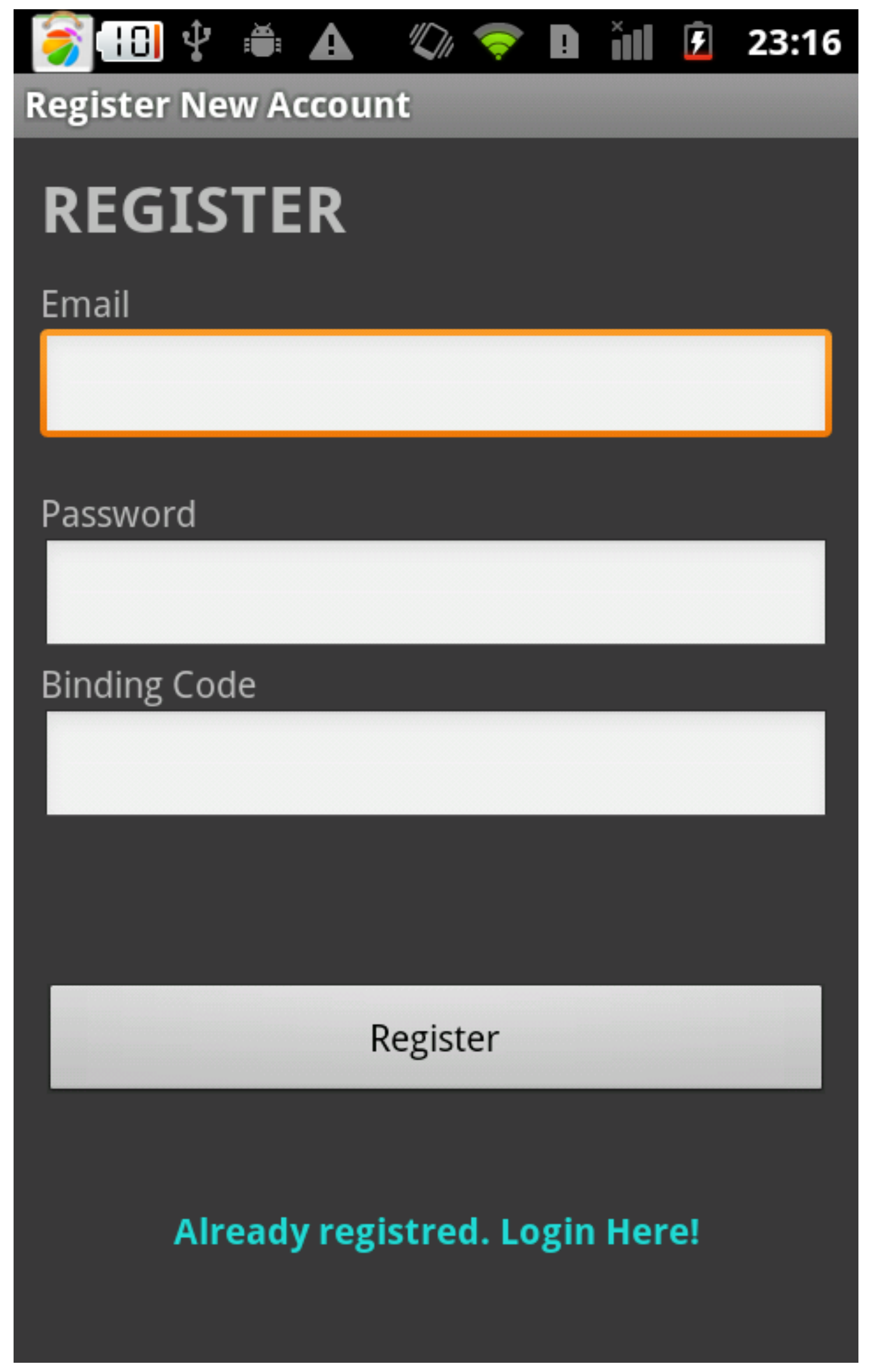
Software Token

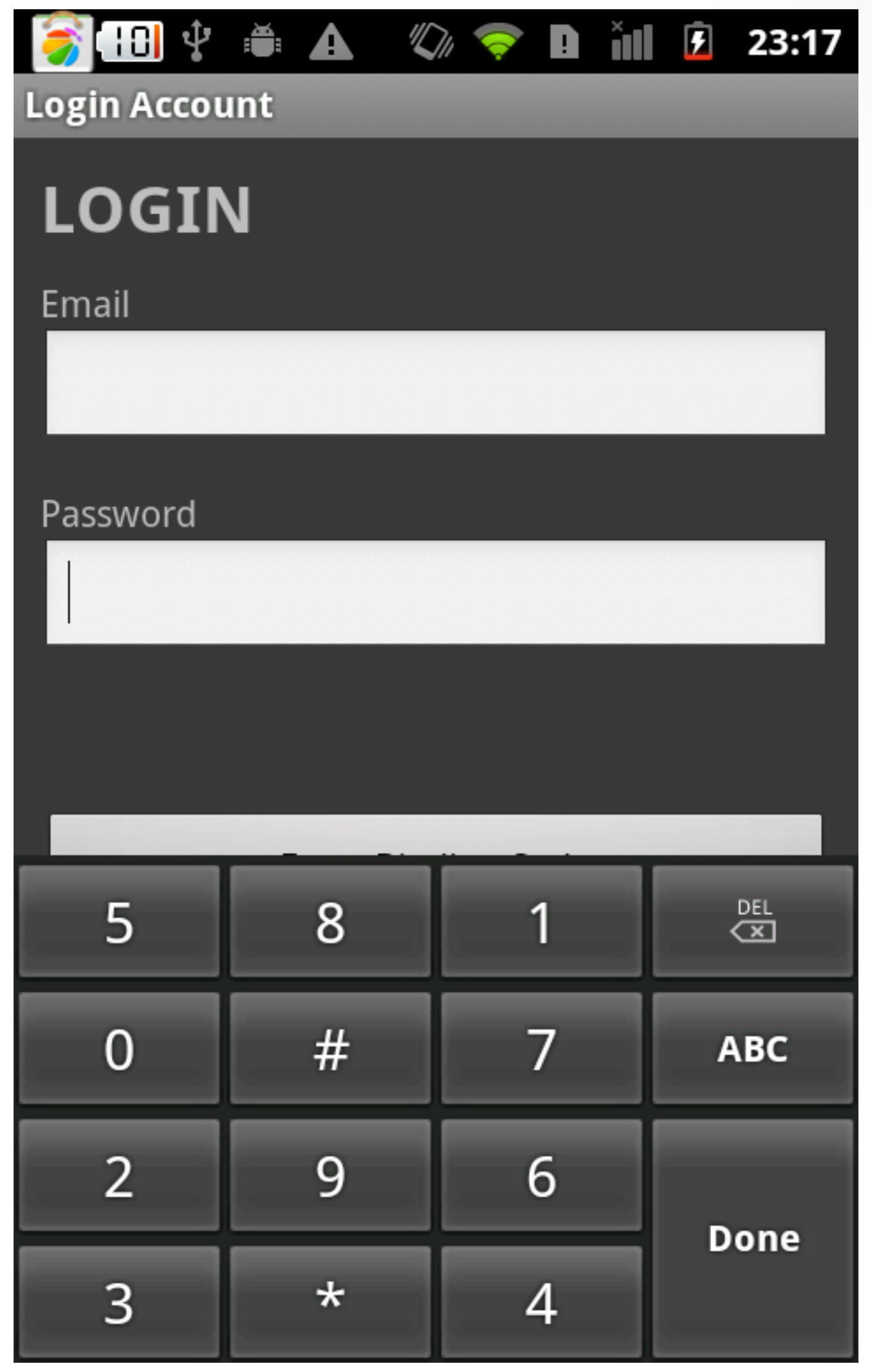
- Software token is based on the same concept of the security token, except there is no physical hardware.

Virtual OTP

- Our OTP uses a model similar to the telephone pad, which consist of number 0 to 9 with # and *. Each time the pad will have the number generated in random position, the user will then enter the password with a touch screen device.
- When Registering, the user needs to create a binding code; it is needed for the application to properly function. The code is used to generate the random pattern.

KEAN UNIVERSITY World-Class Education

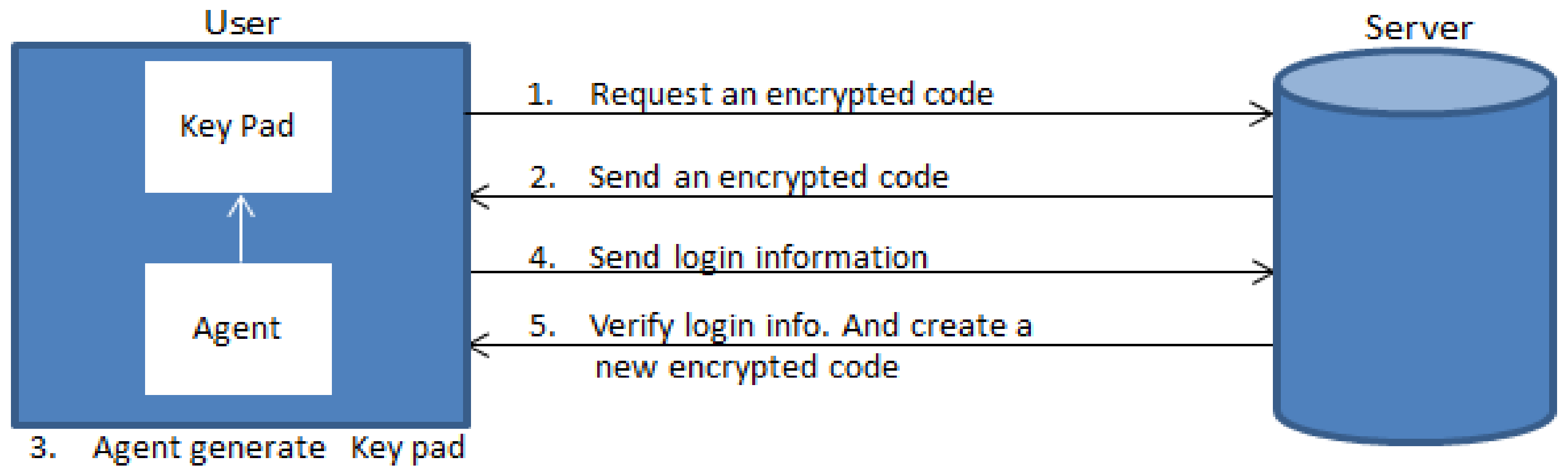




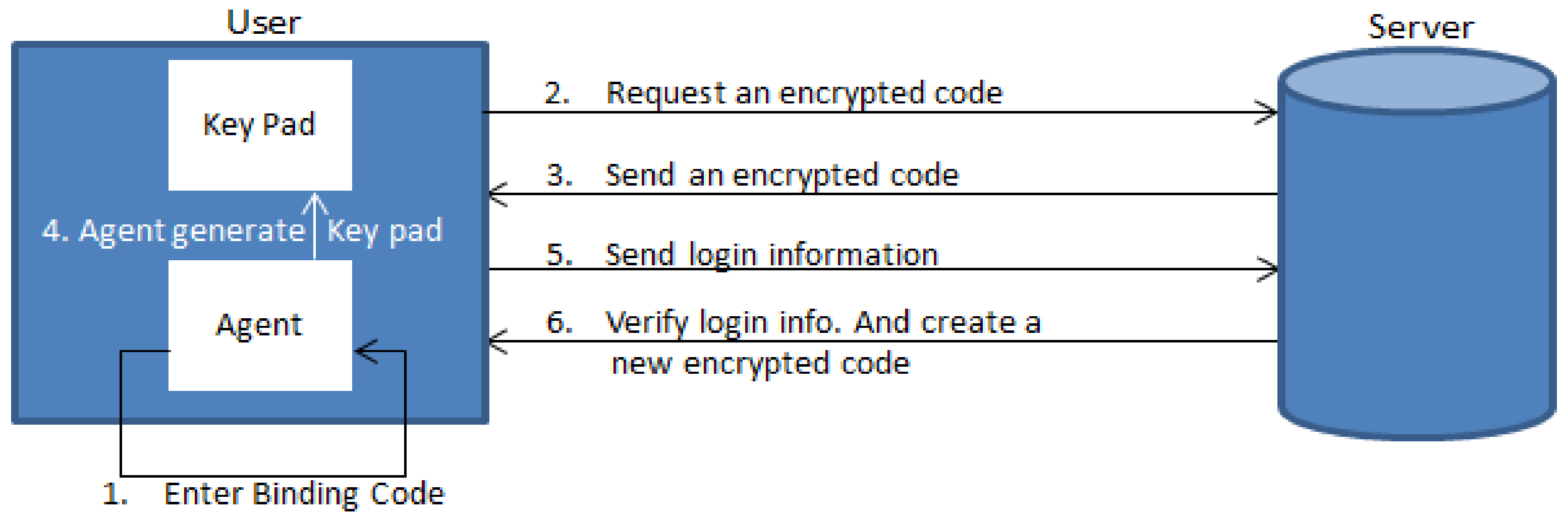
Virtual OTP Process

- If a user is using their own device to log in, the binding code is embedded in the device when registered.
- If using a public device, binding code is needed to be generate the correct pattern so the server be able to decrypt it.

Private Device


User
Server
Key Pad
Agent
1. Request an encrypted code
2. Send an encrypted code
4. Send login information
5. Verify login info. And create a new encrypted code
3. Agent generate Key pad

Public Device


User
Server
Key Pad
4. Agent generate Key pad
Agent
2. Request an encrypted code
3. Send an encrypted code
5. Send login information
6. Verify login info. And create a new encrypted code
1. Enter Binding Code

Strength of Virtual OTP

- Our virtual OTP is highly secure, it can prevent hijacking and key logger.
- The application is highly portable, it can be used on computer, tablet and smart phone.