# Overview

Financial and banking service providers use SMS in the fight against cyber fraud. Each time a consumer wants to perform a transaction, a password is sent to the consumer’s phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired. In this scheme, the lack of encryption on SMS messages is an area of concern. In this experiment we evaluate two solutions to hide the actual password from unauthorized eyes: Secret Formula and Secret Image. In the secret formula scheme, we apply a user-selected, yet secret function to the SMS code to make a password out of it. In the secret image method, we use visual cryptography principles to hide the SMS code.

The experiment has two parts: registration and authentication. Participants are expected to register with each method, try to authenticate 5 times and then fill out a survey about their experience. The registration is web-based and for the authentication part we use a cell phone simulator.

# Registration

 The user registers to secret formula or secret image method by going to http://nisl.cs.gmu.edu:8000/Camouflage/UserRegisteration.aspx.

## Secret Formula



Secret formula has 4 optional parts:

Pre-String: A string that you add to the beginning of your password.

Function 1: You choose one operator (+, - , \*, /) and an Integer operand.

Function 2: You choose one operator (+, - , \*, /) and an Integer operand.

Post-String: A string that you add to the end of your password.

When a user who has chosen the secret formula method initiates a login, he/she receives a 4-digit code via SMS. The user applies the secret formula to the SMS message to create the password. Here is an example:

* SMS password: **1234**
* Pre-String: “$”
* Function 1: x 2
* Function 2: + 100
* Post-String: “&”
* Secret Formula: “$” + (<random number> \*2 )+100 + “&”
* Password Calculation: “$” + ( 1234 \* 2 ) + 100 + “&”
* Actual password: **“$5468&”**

## Secret Image



In Secret Image method, the user needs to transfer the secret image to the his/her cell phone and let the system know where the secret image is stored on the cell phone. For the purpose of this experiment, we use cell phone simulator and we have pre-loaded the secret image to the simulator.

# Authentication

After registering with one of the methods, the user uses a cell phone simulator (Openwave V7) to try the method. For this purpose the user must go to <http://nisl.cs.gmu.edu:8000/Camouflage/> and depends on the registration, user will see different challenges.

|  |  |  |
| --- | --- | --- |
|  |  |  |