Handling IDN Homograph Attack using Facial Expression Password

Kalpana, Preeta Rajiv Sivaraman, Rishabh Kumar

Abstract: ***With the advancement of technology and its applications in diverse areas, people are able to get access of the desired information, exchange ideas and connect with the world. But one of the areas of concern is that user shares personal information for example images, videos, sharing location etc. on various social networking websites very frequently. Another important aspect is sharing financial information for various activities such as payments and purchases which is misused using phishing attacks. There are different variety of attacks that one may come across. The objective of this paper is to make people aware of the increasing fishing attacks such as IDN and how using latest authentication technique of Facial Recognition system one record various facial expressions to secure himself from such attacks since only the user is aware what facial expression he/she has recorded for a particular website.***

Index Terms: Phishing, IDN, Facial Recognition System.

INTRODUCTION

A bug called heart bleed open up a breach allowing hackers to steal any information which is protected using password using cryptographic software, so it is advised to the public to alter passwords for different accounts and change it character changes (like a "1" in place of an "I"). But suppose a bad link looked completely normal, or perfectly mimicked the one that you log on. In that case the user will not be able to recognize that the link is not the original one. In that case the user, the user will enter his login credentials and unfortunately he is redirected to the fishing website, the objective of such attack is not just to steal user credentials but also to perform malware attack onto user systems.

A) Problem statement

The phishing emails and websites appears to be same as that of the legitimate organizations hence the user accidentally logs in to such website as a result of which the user loses personal/financial information. Using multifold security Techniques like security toolbars and Facial Recognition Techniques such attacks can be avoided.

B*) International Domain Name (IDN):*

It is a domain name that uses non Latin characters such as Chinese, Cyrillic, Greek or Japanese letters. It was introduced in order to attract the owners of the websites to create the domain name in their own native language. But, unfortunately this technology is misused to create a spoofed link that can be created using a domain that uses a mix of Latin and non-Latin characters. Because there are many lookalike characters between different alphabets, it's nearly impossible to determine a fake domain on appearance alone. Hackers can take advantage of this to execute a Unicode domain phishing attack, also referred to as an internationalized domain name (IDN) homograph attack. For example, using ASCII alphanumeric characters a fake URL can be created using symbols that are akin to each other. Every so often the letter **q** may be confused with **o**, or **g** with **0**.
http://www.g00gle.co.uk
https://www.ca.com/

The mentioned domain looks like the domain for CA Technologies' website, but it was actually created by Alex Holden of Hold Security, Inc. using Cyrillic characters where the "ca" in the domain is made up of the Ukrainian letter for "s," which is represented by the character "c" in Russian and Ukrainian, as well as the Ukrainian letter "a." According to a research conducted by Farsight Security in June,2018,Cryrillic(Russian Alphabet) characters are the most used characters for IDN Homograph attack. The reason being its close likenesses to normal Latin and shared character pool.

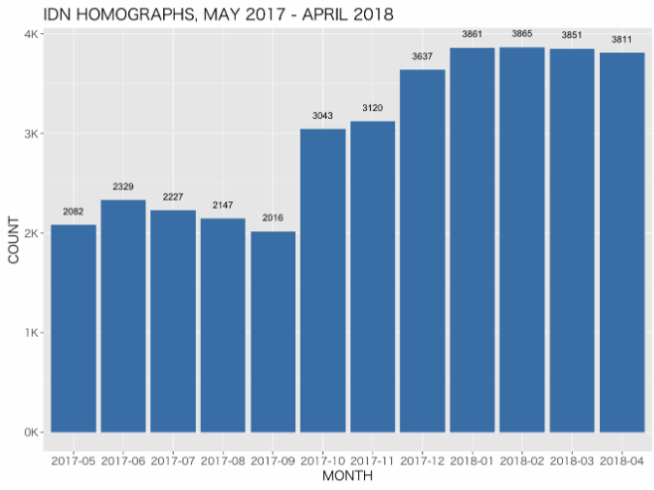


Fig 1 IDN Homograph attack

Revised Manuscript Received on July 5, 2019

Kalpana, Department of **BCA**, Jims Engineering Management Technical Campus, Greater Noida, Uttar Pradesh, India,
Preeta Rajiv Sivaraman, Department of BCA ,KCC Institute of Legal and Higher Education ,Greater Noida ,Uttar Pradesh ,India
Rishabh Kumar, Department of BCA ,Jims Engineering Management Technical Campus, Greater Noida, Uttar Pradesh ,India

Retrieval Number: B10880782S719/19©BEIESP
DOI: 10.35940/ijrte.B1088.0782S719

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It has been observed that the use of combined Latin and Cyrillic characters seems to have been the chosen method of masking an IDN homograph attack, also using combination of Latin/Greek characters, and Greek Cyrillic and Latin characters. Such kind of script is called Intra –Label mixed script homograph which allows more difficult to spot homographs.

The diagram is based upon the study conducted by Farsight Security Team regarding the popularity of homograph attack using data between the period May 2017 and April 2018 which depicts that 35,989 domains which tried to imitate those 466 brands with lookalike domains, used confusable characters, and looked like an attempted homograph attack

II SOLUTIONS

A. Role of Toolbars

Security Toolbars: Security toolbar help to display the security information about the website. There are types of security toolbars available in the market which are discussed as follows

1. Spoof Stick -> The role of the spoof stick is to display domain name of the website.
2. Netcraft Toolbar ->It displays supplementary site data including the site's registration date, popularity, hosting country and other important information.
3. Trustbar: It displays information in a simple way and also helps to improve security features. It has button, that the user may click in case he/she suspects a fraud
4. Spoof Guard ->Here, calculation of a spoof score is done. It is performed for the web page based on a set of detection rules using heuristic technique. It then displays different colors to indicate whether the page is analyzed is secure or not. But the question arises that can we rely on such tools or not.

The solution to stay safe from such security attack is to install Chorme and Firefox extensions and for a site If you are an owner of a website then Dnstwist can be used, that is Python script, that allows seeing sites that are trying to harm others by looking like original website. It uses a domain name as input and then uses various algorithms to generate derivative domains that could potentially be used for phishing, typo squatting, or corporate espionage.

B. Look for Punycode to avoid Unicode domain phishing

Luckily, most browsers can warn you about these URLs and display them in Punycode. It is a method of transforming Unicode to the limited ASCII character subset used for internet host names. Punycode-encoded IDNs begin with the prefix "xn--"to indicate the start of a Punycode-encoded label. In order to be safe from such kind of attack change the settings to always render IDNs in Punycode. Type "about:config" into the address bar, then use the search bar to look up "punycode." Double-click the entry "network.IDN_show_punycode" to change it from "false" to "true."But it has been observed that the different type of toolbars have their own advantages and limitations. Hence applications needs to be developed in this regard to provide better security.

III. FACE RECOGNITION SYSTEM

A. Need:

The latest trend in this regard is to use biometric authentication that makes use of the body characteristics such as fingerprints to uniquely identify each user in place of remembering the password. Another innovative trend is Face Recognition System which detects and tracks physiological features.

As we can't rely on passwords/passcodes due to the fear of being lost or stolen. Sometimes people write their password on a piece of paper which may be caught by somebody else and misused. Also the length and memorability is an issue. Hence using only password for security is not the solution to the security problem. Another technique to provide security is to use biometric system which is much easier and safer to use. But the problem is not yet resolved as biometric technique has its own advantages and limitations. Hence using only one layer of authentication, is not sufficient. Adding second layer of authentication is a solution as it will be difficult and more time taking to bypass two level authentication. Biometric has become a distinguished method in identity authentication due to uniqueness of individual's biometric also it cannot be forgotten or stolen. As a result of which, face biometric is used in multiple applications.

Limitations of biometric(unimodal) for identification:

1. Occurrence of Noise in the identified data: Due to unfavorable conditions such as less or more brightness while capturing the face of the user, it becomes difficult to recognize a face.

2. Intra-class variations: These variations occur when a user is imperfectly interacting with the sensor for example improper facial pose.

3. Another problem occurs when people are unable to provide a standalone biometric credential because of certain illness or disabilities. Hence the authentication system is unable to obtain significant biometric data for some users.

B. Steps in Face and Expression Detection Model

Although, there are different biometrics systems such as fingerprints, palm print, iris detection technique We propose a two level detection model that recognizes the facial expression of a user after detecting the face for verifying identity and authentication. This model takes the advantage of the fact that the human face contains lots of expression such as angry, sad, neutral, happy, surprised etc.

This system doesn't require touching the person or an equipment as face can be detected from a small distance. Our detection model talks about the verification of the user by extracting features of the user and then matching the expression that the user has registered with that particular website. This step is performed once the user has entered password. This mechanism can be used by various websites such as Facebook to provide security to its users and hence phishing attacks can be avoided.

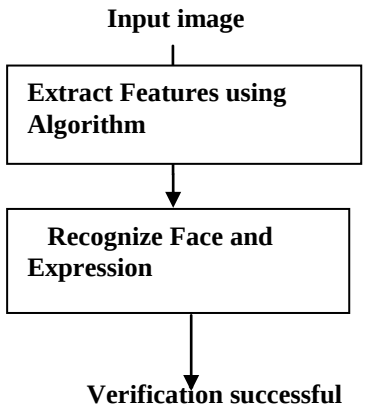


Fig 2 Steps in Verification Process

IV. PROPOSED ARCHITECTURE FOR AUTHENTICATION

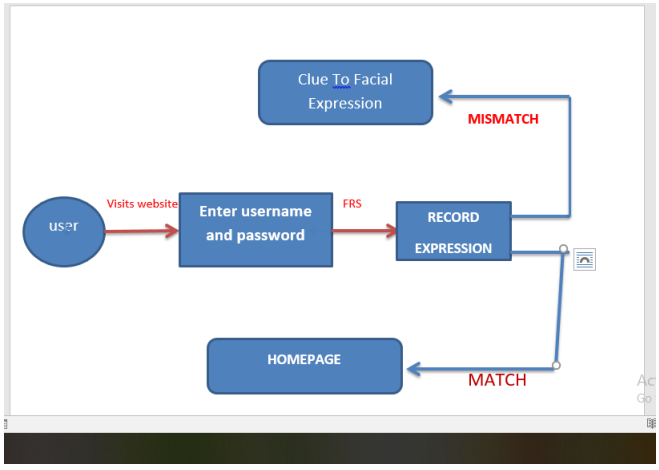


Fig 3 Block Diagram of Proposed Authentication system

A. Working

As per our proposed block diagram, as soon as the user makes an account on any of the websites a specific expression may be recorded with that particular website and next time when the user logs in to the website after entering the id and password, the login page can be redirected to another level of authentication for facial recognition, where the facial expression of the user is matched with the earlier recorded expression. The user will be directed to the homepage only if the facial expression gets matched and in case the match is not correct, the user is asked to answer certain set of previously recorded questions corresponding to that expression. Since, only the user is aware of the expression that he/she has recorded for each website ever the morphed face of a person will not work here since it requires the corresponding expression. Here, we take advantage of different facial expressions as sad, happy, angry, confused and neutral for authentication in different websites. We propose to work on face biometric system by combining physical and behavioral biometric attributes in the model, that supports its system to overcome the limitations of each other. Firstly, authentication is performed to identify the user's face. Secondly, facial expression is integrated which provides another level of authentication. In a very few cases where coincidentally people have a resemblance of facial appearance, working only with Facial Recognition system will not work. Since, the system may provide false result by recognizing a very resembling face with the registered user's face. In order to overcome the problem that may occur in such cases, by including facial expression, it will be very difficult to predict what facial expression a user has recorded for that particular website. If the attacker tries to apply hit and trail method for expression, a restriction on the number of attempts can be applied and on exceeding the limit, a message regarding the fake login can be sent on the registered mobile number. This type of system has the ability to differentiate people even if face of the user is morphed using the available technology.

B. *Algorithm*

In order to detect face, different algorithms are there. Every algorithm takes into consideration certain attribute of the face by extracting the features such as contours, skin color, presence of facial hair. Every algorithm has its own pros and cons. These all algorithms suffer from certain limitations.

Basically, an image of the face image is only a collection of different intensity of light and color. There is wide variation in the images due to different shapes of the faces such as round, square, oval. Also the pigmentation pattern on the face such as pigmentation near eyes, cheeks or chin is different. Using various algorithm these features are analyzed. One of the algorithm to detect a face, devised by Viola and Jones called Haar uses haar like features. In order to detect objects, haar features are scaled independently in vertical and horizontal direction. In a detection window a Haar-like feature considers neighboring rectangular regions at a particular location and performs the sums of pixel intensities in different regions. After that, the calculation of the difference between these sums of intensities is performed. Now, in order to find different subsections of an image, the calculated difference is used. The description of features is as follows:

Total feature:14
Edge features: 4,
Line features: 8
Centre-surround features:2

In order to detect objects, these features can be scaled in horizontal and vertical directions

1. Classifier is trained using decision tree rejecting non-object patters Detection is done by moving a window over the image.

2. Now the various stages of classifier are labelled as positive or negative based on current location of window Depending upon the algorithm, the following inferences can be made: positive value - face identified or negative value - face not identified.

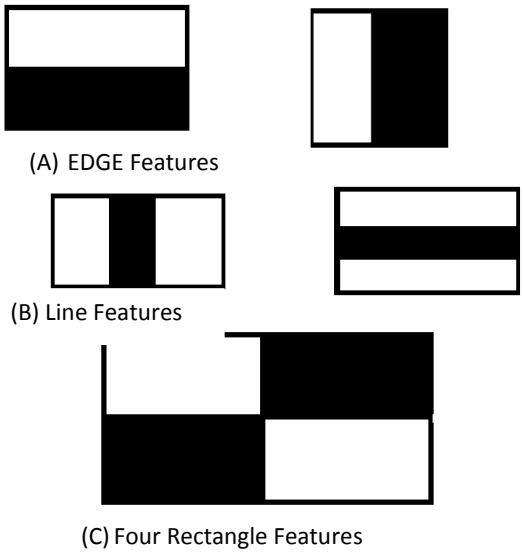


Fig 4 Feature Extraction

V. INFERENCES

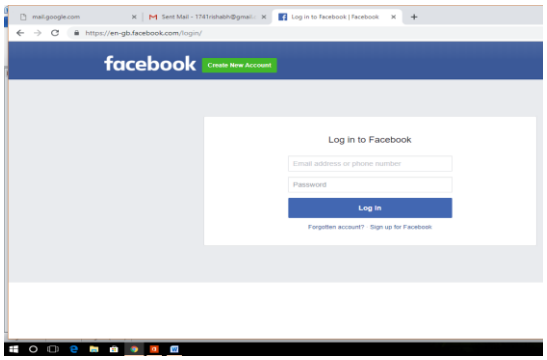
Based on our study we have proposed a login page for Facebook where the user can record any of the expression for along with the password for better security. The fig 6 displays the different types of expressions while figure 7 is the proposed login page for the Facebook Login.

a)Happy

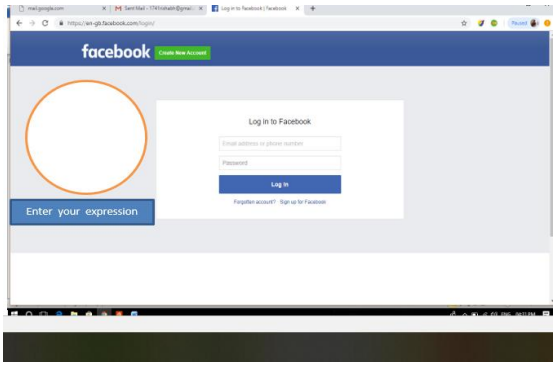
b)Neutral

c)Angry

Fig 5 Different Expressions



a)Facbook Login Page



b)Proposed Login Page

Fig 7 Proposed Facebook Login Page

VI. CONCLUSION

This paper talks about how Facial Recognition System can be used along with the traditional method of authentication. There are different techniques for Facial Recognition, depending upon the nature of the problem a particular method can be adapted. This type of authentication model can be used in various applications to provide a two-way security. This type of authentication cab also be used in various day to day applications such as opening the door as well as for people with physical disabilities who can't speak or can't see. The industry must spread awareness among the people about the various phishing attacks that may harm the people. People need to know the Cyber Laws which covers the broad area of usage of internet and information security. One must share personal and financial information judicially over the internet using the various security measures. Even if one becomes the victim of such kind of attack, it must be reported immediately so that necessary action can be taken against such crime.

REFERENCES

1. Min Wu, Robert Miller and Simson Garfinkel, " Do Security Toolbars Actually Prevent Phishing Attacks? " MIT Computer Science and Artificial Intelligence Lab,32 Vassar Street Cambridge, October ,2005.
2. J.D. Tygar and Rachna Dhamija ," The Battle Against Phishing: Dynamic Security Skins" , ACM Symposium on Usable Security and Privacy, July 2005, pp. 77-88
3. .Kasturi More, Prajakta Kadam, Anjali Jadhav and Dilip Dalgade,"Face Authentication Application for Social Networking Site ",International Journal of Computer Science and Mobile Computing Vol. 4, Issue. 3, March 2015, pg.430 – 433
4. Balamurali Kaliyaperumal and Rajasekaran.M ," Application Authentication:Facial Expression Password ",iieng conference proceedings,2015.
5. Pengqing Xie ," Facial movement based human user authentication", University Digital Repository Iowa State University Ames, Iowa ,2014
6. Or Katz , "A New Era in Phishing — Games, Social, and Prizes", May/2018.
7. Qian Cui, Guy-Vincent Jourdan, Gregor V. Bochmann," Tracking Phishing Attacks Over Time, International World Wide Web Conference Committee (IW3C2), ACM 978-1-4503-4913-0/17/04, Perth, Australia,April 2017,.

AUTHORS PROFILE

Ms. Kalpana
Assistant Professor, Department of BCA
Jims Engineering Management Technical Campus, Greater Noida, Uttar Pradesh, India .She is M.Tech in Computer Science and B.E in Information Technology from PDM College of Engineering affiliated to MD University Rohtak .She has more than 8 years of Teaching Experience. She has published serveral Papers in National and

Preeta Rajiv Sivaraman
Assistant Professor, Department of BCA
KCC Institute of Legal and Higher Education Greater Noida, Uttar Pradesh, India.She is M.Tech in computer Science(Pursuing),MCA, B.Ed having 11 years of corporate and teaching experience. She has published various papers in National Journal. Her areas of interest Big Data, Software Engineering and Artificial Intelligence.

Rishabh
Student, Department of BCA
Jims Engineering Management Technical Campus, Greater Noida, Uttar Pradesh, India. His areas of interest are Problem solving using Programming, security in social networking.