Evaluating Usability Factors In Different Authentication Methods Using Artificial Neural Network

Mapayi, T.
Department of Computer Science
University of KwaZulu-Natal
Durban, South Africa
tmapayi@yahoo.com

Olaniyan, O. M. & Isamotu N. O.
Department of Computer Science
Bells University of Technology
Ota, Nigeria
[tayoolaniyan2001; nehehandsome } @yahoo.com

Raji Shakirat.O.
Department of Information Systems
Faculty of Info. & Com. Technology
International Islamic University
Malaysia.
Peacefultosin@hotmail.com

Olaifa Moses S.
Dept of Computer Systems Eng.
School of Info. & Com. Technology
Tshwane University of Technology
Pretoria, South Africa
newmososaifa@yahoo.com

ABSTRACT
The human factor is often described as the weakest part of a security system and users are often identified to be the weakest link in the security chain. Likewise, authentication is a cornerstone of most security systems today, and most users interact with these mechanisms on a daily basis. Usability of the authentication mechanisms has seldom been investigated as a result little has been said about suitable evaluation model that considers usability and security. Over the years it has proved extremely demanding to merge usability with security in the choice of authentication methods. This somewhat mutual exclusivity of the two terms has placed users of these authentication methods in perilous positions. This research work develops a model that can help to ascertain the usability of the different authentication methods using artificial neural network.

Keywords: Authentication, Usability, Human Factors, Security Chain, Artificial Neural Network.

1. INTRODUCTION
Human factor is often described as the weakest part of a security system and users are often identified to be the weakest link in the security chain. Likewise, authentication is a cornerstone of most security systems today, and most users interact with these mechanisms on a daily basis. Some mechanisms can operate as a one-step procedure of identification or verification only. Authentication mechanisms have been described to be of three types, namely:

i. What you know or knowledge-based systems: a concept which has traditionally been embodied in Personal Identification Numbers (PINs) and passwords.
ii. What you have or token-based systems: a concept commonly related to smartcards.
iii. Who you are or systems based on biometrics: the notion related to biometric authentication.
These traditional authentication techniques have been used to provide a secure means to keep information secure. However, as our information rich society becomes heavily reliant on greater measures of security to protect critical information and data, it has proved extremely demanding to consider the issue of usability within the different authentication approaches. Usability can be defined as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” (International Standard Organization (ISO)). Security usability is concerned with the study of how securing information should be handled in relationship with the different human users. According to [3], authentication methods are needed and since security mechanisms are conceived, implemented, put into practice and violated by people, human factors should be taken into account in their design.

Usability of the authentication mechanisms has seldom been investigated as a result little has been said about suitable evaluation model that considers usability and security. The aim of this research is to develop a model for evaluating a fully functional usable authentication method using artificial neural network due to its pressing urgency.

2. RELATED WORKS

According to [6], specific risk and complications associated with password authentication were highlighted. He also proposed an authentication method based on neural network using feed-forward architecture. The specific risks he highlighted includes: technical (brute force), discovery and social engineering. In the brute force attack, two methods can be used, (a) Attempting passwords against the system, but this is easily stopped with account lockouts. (b) An offline attack against the password hash file. This is processor intensive search through the entire password key-space, calculating and comparing hash values of potential passwords to the values in the stolen hash file.

Password may also be compromised by discovery. Forms of password discovery may vary and include interception of a script file, an exploit on another system, a Trojan program capturing keystrokes, or the discovery of default passwords associated with other system or programs. The primary defense against discovery is proper system design rules that do not allow discovery of passwords through scripts or default system accounts. Social engineering represents an attempt by an intruder to elicit password and account information from a user. This attack is exogenous to the computer system in question, coming via phone, fax, email or causal contact. [6] used artificial neural network to design a very efficient, robust and simple security system having the intrusion detection capability. He achieved this by splitting the encrypted information in two parts.

One part can be stored with security environment whereas other part can embed in to any user-friendly device. According to [7] in her paper, she defined the term user-centered security to refer to “security models, mechanisms, systems, and software that have usability as a primary motivation or goal.” She also emphasized the importance of focusing on the users in the development of secure systems. This is because when user’s mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. She also identified three basic challenges facing user centered security as well as identifying ways in which these problems are being circumvented. The problems include:

1. human and social relationships to usable security,
2. technical challenges best attacked with research, and
3. further difficulties with implementation and deployment.

These troubles can be resolved by Human Computer Interaction techniques and some usable security principles to take us to the next level. According to her research expert evaluation and user testing are producing effective usable security today. Principles such as safe staging, enumerating usability failure risks, integrated security, transparent security and reliance on trustworthy authorities can also form the basis of improved systems.

[1] took an exception to the popular opinion that “the human factor is often described as the weakest link in the security chain” by suggesting that, rather than blaming users, we should understand the roles and demands placed on them by security systems. He laid emphasis on traditional password authentication highlighting various problems and proffering solutions to these problems. Some of the problems he discovered were based on the fact that users tend to choose short and/or guessable passwords, users forget their passwords, users are often willing to tell their passwords to strangers who asked for them.

He however carried out research that shows that users are not to be blamed entirely for many of these problems because users are often the inheritors of system defects, poor designs, incorrect installations, faulty operation, and bad management. Other problems supposedly caused by users happen because users are often faced with remembering dozens of passwords or PINs, but human memory is brief and easily confused. Also users are supposed to create passwords that cannot be guessed. However, our memory systems are particularly weak at remembering meaningless content. Some of the solutions to the abovementioned problems according to [1] includes: Users should also be educated about their password choices; reduce the memory load placed on users as it is well known that cued recall, where users are prompted for the information they must remember, is more accurate than free recall.
[5] developed a model for evaluating the human impact that password authentication issues are having on the security of information systems. This was done by carrying out a survey. The survey helped to evaluate user practices in determining passwords as well as determine vulnerabilities produced through user actions. A large federal agency (US government agency) was used as the case study. The survey was followed by testing the usefulness of individuals customizing their passwords utilizing meaningful data and mnemonic devices in password development and also determining the human impact that password authentication issues have on information security. The findings indicate that human error associated with password authentication can be significantly reduced through the use of passwords comprised of meaningful data for the user and that meet the information technology community requirement for strength of password.

[10] frowned at the use of alphanumeric password form of authentication because of its inherent disadvantages. The research also help to deduce that graphical passwords (i.e., passwords that are based on images rather than alphanumeric strings,) which has led to greater memorability, decrease in the tendency to choose insecure passwords and increase in overall password security also has some disadvantages. These include needing simple, artificial images, predefined regions, and consequently many clicks in a password. In the paper a new design was explained which improved on the previous approaches in the areas of security, learning, performance, and retention. In the proposed system any image could be used and it does not need artificial predefined click regions with well-marked boundaries – a password can be any arbitrarily chosen sequence of points in the image. From the results from various users who tested the system some of the advantages of the system were: It is easy to obtain large passwords spaces; furthermore, in the experiment it appears that users rarely chose points that were within the tolerance around the click point of another participant. That is, people were not strongly drawn to a few salient areas that an attacker might guess. Finally, there is currently no efficient way of creating dictionary attacks against the system.

[11] Summarizes the advantages and disadvantages of biometric authentication in terms of its usability and security. According to the writers, biometric authentication methods are better than traditional methods since these methods are solely based on properties that can be forgotten, disclosed, lost or stolen. Biometrics was defined as automated methods of identity verification or identification based on the principle of measurable physiological or behavioral characteristics such as a finger-print, an iris pattern or a voice sample. It also sheds light on the pros of biometric authentication. They authenticate the user. Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords.

Most biometric techniques are based on something that cannot be lost or forgotten. While the advantages of biometric authentication look very attractive, there are also many problems with biometric authentication that one should be aware of. Biometric systems still need to be improved in the terms of accuracy and speed. Also not all users can use any given biometric system. People without hands cannot use finger-print or hand- based systems. Visually impaired people have difficulties using iris or retina based techniques. As not all users are able to use a certain biometric system, the authentication system must be extended to handle users falling into the “Failure To Enroll” category. This can make the resulting system more complicated, less secure or more expensive. Biometric data are not considered to be secret and security of a bio-metric system cannot be based on the secrecy of user’s biometric characteristics. However according to the writer, sometimes biometric authentication systems replace traditional authentication systems not because of higher security but because of higher comfort and ease of use.

[12] proposed a new graphical password scheme using dynamic block-style that aims to balance the problem between usability and security. Fuzzy logic methods were used to enhance the usability by allowing certain degree of tolerance during authentication. The proposed scheme is able to provide larger password space and reduces registration and authentication time. The results of the experiment was, in terms of usability, the registration and authentication processes are simple; users only need to key in their username and click on the password (image). Selection of the image also affects the security and usability of the system. Simple images increase the usability, which are more users friendly and memorable. The users did not get confused during the system test phase. Besides, these processes are easy and fast. Users are allowed to proceed to their actual tasks with minimal time. A degree of tolerance is allowed to increase the system usability. Furthermore, the user interface of the system is simple and understandable to users on the first view. Lastly, the instructions are clear to guide new users on how to use the system.

[9] explained the positive relationship between security and usability. According to the paper, security is aimed at making undesirable actions more difficult while usability aims at making desirable ones easier for the user, it may also be true that improving one also improves the other. A usable system will minimize unintentional errors, while a secure system will aim at ensuring that undesirable actions in a system are prevented or mitigated. A security usability threat model was also developed that focused on legitimate users’ mistakes that may compromise the system as against standard security threat models which focus primarily on malicious attackers who may or may not be legitimate users.
The concept of usage scenarios (usage scenarios are actions that are desirable to stakeholders of a secure system) and threat (negative) scenarios (threat scenarios are actions that are not desirable and hence the system should not allow them to happen) were used to understand and identify both system and external elements that are threats to a system’s usability, security, or both.

[2] summarized current research on the usability of security mechanisms and discussed options for increasing this usability and the effectiveness of these mechanisms. According to [2] usable security is not simply an issue of ‘fixing’ user interfaces to current mechanisms; rather, a change in how individuals, organizations and governments think about security is required. Effective security has to take into account the needs of all stakeholders, acknowledge that their needs sometimes conflict and find a solution that is acceptable for all stakeholders in ongoing use. However while the paper emphasizes the urgent need to put users’ needs and values at the centre of security design, there is a note of warning: most users are not knowledgeable about security, nor do they want to be. Motivational approaches therefore could be employed to change underlying perceptions about security and a limited set of key behaviors, but they will not motivate the majority of users to become security experts.

[3] presented the usability and security issues of the user authentication methods in the computer security and access control domains. The various methods of authentication were compared in terms of their security and usability. Some of the methods used includes passwords, pins, proximity card, one time generators, challenge response, multifunction card, fingerprint, voice and signature. According to the survey carried out by the writers, one of the methods that scored highest is the multifunction card. It however has the need of a smart card reader as its disadvantage.

3. NEURAL NETWORKS

[3] and [8] explained that neural networks have emerged as an important tool for classification purposes. The recent research activities in neural classification have established that neural networks are a promising alternative to various conventional classification methods.

Artificial neural networks (ANN) are relatively crude electronic networks of "neurons" based on the neural structure of the brain. They process records one at a time, and "learn" by comparing their classification of the record (which, at the outset, is largely arbitrary) with the known actual classification of the record. The errors from the initial classification of the first record is fed back into the network, and used to modify the networks algorithm the second time around, and so on for many iterations. ANNs combine artificial neurons in order to process
A neuron in an artificial neural network is:
1. A set of input values \((x_i)\) and associated weights \((w_i)\),
2. A function \((g)\) that sums the weights and maps the results to an output \((y)\) [8].

4. USABILITY-CENTERED AUTHENTICATION

A usability-centered authentication approach is urgently needed to be able to bridge the gap between usability and security thus satisfying both usability and security goals of the users of authentication systems as describe in the figure below:
5. THE PROPOSED ARTIFICIAL NEURAL NETWORK MODEL

The basic network used for classifying the usability information is a feed-forward back propagation network. The arguments used for categorizing the usability information are:

- Input vectors
- Target vectors
- Size of the layer employed in the neural network
- Transfer function
- Backpropagation network training function
- Backpropagation weight/bias learning function

The first step in creating a feed forward network for usability information is creating a network object this is achieved by using the new function command and its argument are as listed above. The network is then used in training the usability information the network weights and biases are initialized.

There are different methods of training, this includes pattern association or pattern classification, but for the purpose of this research, the network will be trained for regression. The process of training usability information will then require a set of examples of proper network behavior for which the default performance function for feed-forward networks is mean square error.

The network will then apply performance function to determine how to adjust the weights to minimize performance. The gradient will then be determined using a technique called back-propagation, which involves performing computations backward through the network. The back-propagation computation is derived using the chain rule of calculus in most of the training algorithms discussed up to this point; a learning rate will then be used to determine the length of the weight update (step size). The proposed Neural Network Architecture for the evaluation of the usability of the different authentication methods is described in the figure below:

![Proposed Neural Network Architecture Usability-Centered Authentication Evaluation](image)

*Fig. 4: Proposed Neural Network Architecture Usability-Centered Authentication Evaluation*

For this research, a feed forward network is used because of its ability with non-linear classification problems. It is able to form from the high order morphological-extracted features of Authentication factors. Both the hidden and output layers use a continuous network based on the non-linear sigmoid discriminant function.

In a multilayer network based on the nonlinear sigmoid discriminant function. In a multilayer network the number of nodes is determined by the dimension of the feature space physically the hidden layers are inaccessible while the output layer provides user with learning responses after training by adding more hidden layers the network is able to extract higher order status in order to perform more complex task.
Flow Chart
The flow chart of the artificial neural network is described in figure below.

Fig. 5  Flow Diagram for The Application Process
The basic model we use for the study is logistic regression because the responses are in categorical form. Logistic regression analyzes binomially distributed data of the form.

\[ Y_i \sim B(n_i, p_i), \quad \text{for } i = 1, \ldots, n \]

where the numbers of trials \( n_i \) are known and the probabilities of success \( p_i \) are unknown. The model proposes that for each trial there is a set of explanatory variables which can be thought of as being in vector \( X_i \) and the model therefore takes the form:

\[ p_i = E\left( \frac{Y_i}{n_i} \mid X_i \right) \]

The logits of the unknown binomial probabilities are modeled as a linear function of the \( X_i \), that is,

\[ z = \ln \left( \frac{p_i}{1 - p_i} \right) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots + \beta_k x_k \]

We use Logistic regression to predict the probability of occurrence of an event by fitting data to a logistic curve. In logistic regression model, the relationship between ‘input’, \( z \), and the probability of the event of interest is described by the function.

\[ f(z) = \frac{1}{1 + e^{-z}} \]

The variable \( z \) is known as the logit and is usually defined as

\[ z = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots + \beta_k x_k \]

Therefore, it follows that

\[ f(z) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \ldots + \beta_k x_k)}} \]

The model also assumes that \( z \) is linearly related to the predictors.

6. CONCLUSION AND FUTURE WORKS

In this work, the Neural Network based model for evaluating a fully functional usable authentication method has been developed to ascertain usability in the authentication process, thereby providing a suitable evaluation model that considers usability and security. This is because over the years it has proved extremely demanding to merge usability with security in the choice of authentication methods.

In view of the proposed Neural Network based model for evaluating the usability of the different authentication methods, we hope to collect the opinions of a range of computer users through questionnaires as to which authentication approach they find most desirable. The results captured will be used to train the artificial neural network and the neural network model will also be able to predict the authentication approach that achieves both usability and security preferences of various users.
REFERENCES

2. Angela Sasse, M., 2004: "Usability and trust in information systems".
   Christina Bra and Jean-Marc Robert, 2006:” Security and Usability: The Case of the User Authentication Methods”.
5. Manoj Kumar Singh, 2009:”Password based: A generalized robust system design using neural network”.
7. Meral Yay and Eylem Deniz Akinci, 2009:”Application of Ordinal Logistic Regression and Artifical Neural Networks in a Study of Student Satisfaction”.
11. Woo Chaw Seng, Yong Kok Khuen and Ng Liang Shing, 2011:”Enhanced Graphical Password by using Dynamic Block-style Scheme”.

Author’s Biography

Mapayi T. is a doctoral research student at the Department of Computer Science, University of KwaZulu-Natal, Durban, South Africa. He had his BSc in Computer Science at the University of Ado-Ekiti, and his Msc at the University of Ibadan, Nigeria. He is a member of Computer Professionals of Nigeria. His areas of research includes; Biometrics, Computer Security, Computer Vision and Pattern Recognition and ICT for Development. He can be reached through Email: tmapayi@yahoo.com.

Engr. Olaniyan Olatayo Moses (M.SC), a Lecturer at Bells University of Technology, Ota, Nigeria. He teaches computing in the Dept of Computer Science and Information Technology. Engr Olaniyan obtained the B.Tech Computer Engineering degree from the Ladoke Akintola University of Technology, Ogbomoso and a MSc in Computer Science from the University of Ibadan, Ibadan, Nigeria. Presently on PhD degree focusing on Telemedicine Research his other research interest includes Computer Networks and Human Computer Interaction. He can be reached through E-mail: tayoolaniyan2001@yahoo.com

Shakirat O.Raji is a PhD Research Student at Human-Centered Design Group (HCDG), Department of Information Systems, Faculty of Information and Communication Technology International Islamic University Malaysia. Her Main area of Interest is Human-Computer Interaction and part of her interests are Usability Evaluation, Usability Engineering, user Experience as well as Cyber Security. She can be reached through peacefultosin@hotmail.com
Olaifa M. had a B.Sc Computer science from the University of Ilorin and his MSc in Computer science from the University of Ibadan. He was a lecturer at Houdegbe North American University, Benin, Republic of Benin between 2009 and 2011. He is currently at The Department of Computer systems engineering, school of Information and communication technology, Tshwane University of Technology, Pretoria, South Africa. His research area includes Machine Learning (intelligent industrial systems). He can be reached through E-mail: newmosesolaifa@yahoo.com

Isamotu Nehemiah O. is a graduate of Bells University of Technology, Ota, Nigeria. He can be reached through E-mail: nehehandsome@yahoo.com