Evaluation of the Model for Analysing Anti-Phishing Authentication Ceremonies

Edina Hatunic-Webster, Fred Mtenzi, Brendan O'Shea
School of Computing, Dublin Institute of Technology
Dublin, Ireland

Abstract

Phishing takes advantage of the way humans interact with computers or interpret messages. A security ceremony is one way of extending the reach of current methods for social, technical and contextual analysis of security protocols to include humans. It is an extension of the concept of network security protocol and includes user interface and human-protocol interaction. We propose a model with which anti-phishing authentication ceremonies can be examined not only with a technical focus but by including the human into the analysis. The model examines anti-phishing authentication tasks that a human needs to apply, how users process these additional authentication tasks and how these tasks impact the human's decision outcome. We outline the evaluation of the model and propose a ceremony called MultiStep Mutual Authentication (MSMA) that combines PIN, text password and dynamic image feedback as a help to foil phishing attacks. The MSMA ceremony is used as part of the evaluation of the model.

1. Introduction

In spite of significant new legal and technical approaches to fight it, phishing remains one of the main forms of Internet fraud. The number of phishing attacks is still high [8] and is not only increasing, but also the attacks are getting more sophisticated and adaptive. As countermeasures are deployed, phishers are modifying their techniques as well, and phishing continues to be an arms race.

Security researchers have proposed many anti-phishing authentication schemes that suggest: using images for authentication [7],[4],[13]; using digital objects as passwords;or sending one-time password (OTP) tokens out-of-band to the user. However, authentication schemes that are more secure require more effort than traditional username/password authentication, both on behalf of the user and the service provider. If security impedes a user's primary task, the user will probably try to avoid the security measures. The threat analysis and security proofs for these authentication protocols mostly have a technical focus and rarely take into account the human user limitations as a potential threat. When protocols are implemented and used by humans, the underlying assumptions about human-protocol interactions are often susceptible to attacks [5], [12].

Another problem is that while using more complex shared secrets and credentials *increases security*, it significantly *decreases usability* of the resulting interface. Decreased usability makes it more likely that the user will try to bypass the security protocol, leaving them open to *social engineering* attacks, such as phishing. Our specific aim is to research how human users process these additional authentication credentials and whether the additional authentication tasks help to determine if the login page is fake.

In our approach we use the concept of a *security ceremony* to analyse authentication protocols and their effectiveness in combating phishing.

The idea behind the ceremony approach is to deal with *the human factor* explicitly, treating humans as separate entities from their machines, and assuming that they are being subject to social and psychological influences or tendencies. For example, typical password authentication using Hypertext Transfer Protocol Secure (HTTPS) on the Internet is a ceremony where *a human user* needs to type in the *username* and *password* to login to an account; or use a physically protected personal device as out-of-band channels. Human participants are modelled as nodes in the network, separate from the computers and devices they use. Analogous to a computer protocol node, a human node receives and sends messages, sometimes through human computer interfaces, sometimes by human-to-human communication or peripheral devices (e.g. using a smartcard or an USB token) [6]. Unfortunately, human input and output messages are often subject to errors, that are quite regularly treated as arbitrary faults by some of the protocols' correctness models. These errors happen mainly because human nodes have different capabilities than computer nodes.

The complexity of defining a ceremony comes with modelling a human node. The major effort yet to be accomplished in the field of ceremony design and analysis is the modelling of the memory and processing performed by human nodes [6],[16]. Ceremony analysis provides a more complete understanding of the security threats surrounding the use of a protocol by a human than analysing the protocol

alone.

In this paper we build on and expand our previous work on Model for Analysing Anti-Phishing Authentication Ceremonies (APAC) [10], [11]. In order to model the communication processing performed by human nodes in an anti-phishing ceremony we propose a Human Factors in APAC Framework. The framework determines human-protocol interaction features affecting anti-phishing security of authentication ceremonies. We show how to correlate the components of the framework: we design the Model for Analysing APAC that correlates the framework components and will determine principles for minimising human interaction errors in anti-phishing authentication ceremonies. The model can be used to examine anti-phishing authentication ceremonies not only with a technical focus but including the human into the analysis. In particular, the model is used to analyse anti-phishing authentication tasks that a human needs to apply, how users process these additional authentication tasks and how these tasks impact the humans decision-making process and decision outcome: i.e. whether these additional tasks help users to determine if a login page is fake or not. We outline the evaluation of the model and propose a MultiStep Mutual Authentication (MSMA) ceremony that is used as part of the model evaluation.

We begin with a brief overview of related work and differences and features of ceremonies when compared to security protocols (Section 2). We then discuss human behaviour assumptions discovered in many anti-phishing authentication ceremonies (Section 3). In Section 4 we provide an overview of the framework and describe its components. In Section 5 we describe the application of the framework in the Model for Analysing APAC. Section 6 presents the design of a users study for evaluation of the model. It also presents high level design of MSMA ceremony. We discuss our conclusions and future work in Section 7.

2. Related Work

In 2007, Ellison [6] developed the concept of *ceremony*. A security ceremony [6] is an extension of the concept of network security protocol that includes user interface, human-to-human communication and transfers of physical objects that carry data. Ellison argued that a better way for examining the security of a protocol was to consider a security ceremony.

A technique for verification of ceremonies is not an agreed and a straightforward process. In network security systems, Karlof et al. [15] proposed a concept of *conditioned-safe ceremony* which is a ceremony that deliberately conditions users to automatically take actions that protect them from an attack. Radke [16] extends the concept of ceremony to a higher level protocol which uses the underlying protocol as a cryptographic primitive or building block. Gajek et al. [7] did not explicitly use the term ceremony, but their protocol security model specifically included a human into the security proof, as the authentication of the server depends on a human recognising a previously chosen authenticator.

Our framework builds on Cranor's [3] The Human-in-the-Loop Security Framework, which is a communication processing model in which a communication receiver is a human user. The communication sent triggers some behaviour that depends on the outcome of several information processing steps taken by the receiver, the personal characteristics of the receiver and the possible communication impediments. The Human-in-the-Loop Framework is not a precise model of human information processing but it provides a systematic approach for identifying potential causes for human failure. It builds on Wogalter's Communication-Human Information Processing Model C-HIP [20] model, adapting it to better fit computer security scenarios. Our approach differs from Cranor's as we show how to correlate the components of our framework.

Our model, that correlates the components, builds upon prior research in information processing and decision making, Johnson's Theory of Deception (TOD) [14]. The Theory of Deception [14] proposes an information-processing model in which users recognize deception by noticing and interpreting the inconsistencies between the deceptive event and their past experiences. It was originally proposed to understand information processing involved in fraud detection and has been empirically validated in information-intensive domains. The process of recognizing deception is composed of four steps: activation, deception hypothesis generation, hypothesis evaluation and global assessment stage. The last step is to reach the conclusion, where the information is combined to form a single, synthetic assessment of deceptiveness. Researchers have argued that the Theory of Deception can be applied to assess how individuals process a phishing email, and determine whether to respond to it [19], [18].

Login pages used in phishing attacks contain at least some false content and phishers apply deception to fool the user to give away authentication credentials. Hence, Theory of Deception offers a good theoretical framework for investigating the psychological mechanism of human node decision-making underlying the effectiveness of phishing attacks.

3. Anti-Phishing Authentication Ceremonies

Researchers have proposed a number of anti-phishing authentication ceremonies [7],[4],[13], [9]. Most of them have two phases: registration and login. The registration phase involves prompting the user to generate a set of authentication credentials, some of which need to be remembered. During the later login phase, the user may be expected to: retrieve some credentials from memory;

read/write a value from an out-of-bound device; perform a comparison; and then provide it to the authentication ceremony. Hence, human nodes in a ceremony are often required to make decisions that demand significant human abilities and knowledge. Variation of the behaviour of human nodes, such as limited memory, probabilistic memory access, fuzzy comparisons [6], etc. introduces additional flaws in a ceremony. Recognising these flaws could lead to improved ceremony designs.

3.1. Human Behaviour Assumptions

One of the ceremonies we analysed was Gajek's et al. *Provably Secure Browser-Based User-Aware Mutual Authentication over TLS* [7]. The ceremony specifically considers the user and the browser as protocol participants, and ties the user's authentication to the TLS secure channel. The server identifies the browser on the basis of client certificates, ensuring that the server establishes a secure channel to the browser. However, it does not authenticate the user. In order to prove its identity to the user, the server sends a Human Perceptible Authenticator (HPA) [7], e.g. a personal picture or a voice recording. The authenticator was chosen at the registration phase. The user has to recognize the authenticator at the login phase. Verification of server certificates (and the underlying public key infrastructure) and any security indicator (e.g. URL, padlock) is irrelevant. Finally, the user authenticates himself/herself to the server, using a password.

A few commercial variations of these authentication protocols are available, where the server sends a Human Perceptible Authenticator in order to prove its identity to the user. Some offer a choice of images, puzzles etc. Some combine images with the text based passwords. Investigation of these ceremonies reveals a number of issues arising from assumptions as to how a human is supposed to use the protocol as well as the protocol implementation.

The main assumptions made about human node behaviour in reviewed ceremonies and their effect on human-protocol interaction, are summarized in Table 1 and described in detail below. Assumptions and issues that could result from these assumptions are as follows:

- *The user will expect a HPA as part of the authentication ceremony.* This assumption implies that a user is familiar with the ceremony steps and will find it strange to be asked to enter a password without a HPA being displayed. Issue: the login webpage may be *spoofed*; a phisher may trick a user to enter a password in a non-secure manner, so that the secure protocol is never used.

- *The user will wait for a HPA.* Implementing a display of HPA may slow down the execution of ceremony steps. For example, a user may be offered a set of images to choose their HPA from, and their downloading may be very slow. It is assumed that the user will not skip these tasks that potentially slow down his/her primary task offered by a service provider (after the login). But, users are prone to skip a security step if it slows down the primary task [16].

Table 1. Behaviour assumptions in human protocols

Behaviour Assumptions	Issues
The user will expect a HPA	Knowledge of the ceremony Interference Format, Font size, Length Delivery channel, Habituation
The user will wait for a HPA	Distraction from primary task Interference Format, Font size, Length Delivery channel, Habituation
The user is able to recognise a HPA	Cognitive or physical skills Memorability, Interference Format, Font size, Length Delivery channel, Habituation
The HPA is human distinguishable	Cognitive or physical skills Memorability, Interference Format, Font size, Length Delivery channel, Habituation

- *The user is able to recognise a HPA.* It is assumed that the user will switch attention to the right HPA being presented and have the capability to distinguish the correct one. Also, some implementation of the login pages contain service provider's advertisements which may further distract a busy user.

- *The interface will make the HPA human distinguishable.* It is assumed that the implementation of website login forms will make HPAs human distinguishable and memorable. This assumption highly depends on the user interface design that is used to interface with the ceremony.

Based on these and other human node behaviour assumptions and related issues, the components of our APAC framework are defined and described in Section 4.

4. Human Factors in Anti-Phishing Authentication Ceremonies (APAC) Framework

The Human Factors in APAC Framework, presented in Fig. 1, builds on Cranor's [3] The Human-in-the-Loop Security Framework and Wogalter's C-HIP model [20]. Cranor's framework is not a precise model of human information processing, but it provides a systematic approach for identifying potential causes of human failure, primarily by answering questions posed by the framework.

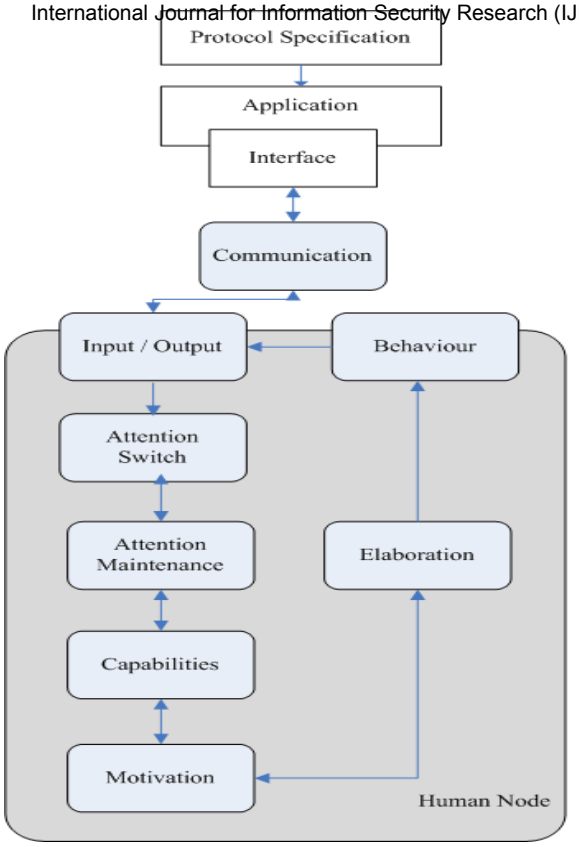

Figure 1. Human Factors in APAC Framework

Different to Cranor, we focus on human security behaviour within *authentication* ceremonies and also we show how to *correlate* the components of the APAC framework. The framework, summarized in Table 2 and described in detail below, includes factors and information processing stages that will impact on anti-phishing related behaviours.

4.1. Framework Components

Communication. The first component of the framework is the communication to the human node, which should trigger an appropriate behaviour in an authentication ceremony. We distinguish three types of communications that are relevant to authentication ceremonies: *recall, recognise, and compare*. They may be combined in an authentication ceremony. *Recall* communications are those that require a user to memorise and recall a specific authentication credential, e.g. recalling a password (and username) in a typical username/password authentication. *Recognise* communications are used in graphical password schemes and in combination with text based (i.e. recall) passwords. *Compare* communication is mainly used in one-time password schemes, where a user is supposed to read/write a value from an out-of-bound device, perform a comparison, and then provide a resulting outcome to

Table 2. The components of the APAC Framework

Component	Factors to Consider
Communication	Recognition Recall Comparison
Input and Output	Keyboard, Mouse, Touch Visual, Auditory, Tokens Out-of-Band Devices
Attention Switch	Colour, Font, Size Motion, Sound
Attention Maintenance	Length, Habituation
Capabilities	Memory, Comprehension
Motivation	Distraction from primary task Convenience, Risk perception Incentives/Disincentives
Elaboration	Automatic responding Cognitive effort
Behaviour	Skipping a required step Predictable Incorrect performing

the ceremony. There are specific issues that may arise from each. For example, humans tend to perform fuzzy comparisons [6], which means ignoring comparisons that cannot be completed because information is lacking or because some other factors suggest a different outcome.

Input and Output. Many anti-phishing authentication ceremonies use other methods than the standard keyboard or keypad to enter credentials. Examples are mouse, touch, visual, auditory, combining with out-of-band devices; combining with a physical token. The type of input affects the level of user's acceptance of the ceremony and hence the anti-phishing security.

The delivery of a communication consists of two steps: attention switch and attention maintenance, and they are the next components in our framework.

Attention Switch. The communication must attract the receiver's attention. In traditional protocol analysis it has been easy to overlook a failed delivery as a source of design error. The assumption was that the communication was sent as per protocol specification. However, the successful sending of a communication does not mean that it was successfully received [5]. For example, a picture used to authenticate a server to the user may not get displayed/downloaded successfully before the user enters his password. Ceremony security analysis needs to make sure that the human node has indeed received the intended communication. The main factors to consider are: *colour, font, size, motion and sound.*

Attention Maintenance. Once the communication has attracted the user's attention, it needs to keep his/her focus *long* enough to be understood. The delivery channel will

have an influence as well. This component is vulnerable to *habituation*, the tendency for users to pay less attention to stimuli they experience frequently, e.g. entering username and password in the username/password fields without considering other authentication factors. Another common behaviour is the user who skips a security step, as he/she is *rushing* to finish a primary task provided by a service provider [16].

Capabilities. An important aspect of authentication ceremony is how newly created authentication credentials are remembered and later retrieved at login. We distinguish two types of capabilities that affect authentication ceremonies: *memory* and *knowledge/cognitive or physical skills*.

Motivation. Motivation plays an important role in how users decide what action they are willing to take. As the compliant ceremony security behaviour often slows down the receiver's primary task, motivation can be difficult to provide. Hence, *risk perception, distraction from primary task and convenience* influence motivation. Risk perception will be determined by the perceived importance of a particular website to a user and also how busy the user is with the primary task.

Elaboration. Elaboration is the process by which users make conscious connections between the cues they observe and previous knowledge. The importance of elaboration in deception detection is supported by prior phishing research [5], [18],[19]. This has its roots in the human psychological tendency to apply rule-based decision making and develop *automatic responses* to situations that are encountered more than once. We tend to classify a communication according to a few key features, and if one or more features match what we have encountered in the past, we usually respond mindlessly with the action that we learned was most appropriate. For example, many users will automatically enter their login credentials on any page which looks familiar and legitimate. This is an important and generally positive feature, otherwise we would spend a considerable amount of time analysing everyday situations. Unfortunately, the phishers have learnt to exploit this predictability of human behaviour.

Behaviour. Behavioural errors can be categorised according to the performance level at which they occur. Mistakes are errors at the rule-based and knowledge-based levels. Humans make them due to picking an inappropriate/deficient rule or incomplete/inaccurate understanding of the system. Slips are errors at skill-based level. They are execution failures, in which the user decides on an action, but the result is not what was intended: e.g. selecting a wrong item on a menu. Behavioural errors may result in a protocol step not achieving the desired goal; users skipping a required step or performing an action incorrectly. Importantly, we need to consider the fact that the user is likely to try to circumvent the excessive security demands in order to accomplish his/her primary task. The *predictability* of behaviour is also very important, as phishers may exploit it.

4.2. Applying the framework

The primary use of this framework is to provide a novel and constructive way of correlating and assessing human-protocol interaction features affecting anti-phishing security of authentication ceremonies. We illustrate this usage of the framework in Section 5 by designing the *Model for Analysing APAC*.

The model correlates the key features responsible for improving the human interface weak points of a ceremony and reducing the success of phishing attacks.

5. Model for Analysing APAC

The main purpose of the Model for Analysing APAC is to determine the *likelihood of a user making an error*, and hence increasing the probability of a phishing attack success. Specifically, the aim is to determine the significance of anti-phishing authentication tasks required to be performed by the user in decision making: i.e. whether these additional tasks help users to determine if a login page is a fake or not.

The model is grounded in the prior research in information processing and decision making, specifically, Johnson's Theory of Deception (TOD)[14].

The human information processing activities are structured into two separate sub-processes: *attention* and *elaboration*. Attention indicates the amount of mental focus given to specific elements of an event or object [19]. In the Theory of Deception, the concept of *activation* is similar to that of attention and consists of allocating attention to the communication details based on the presence of discrepancies between what is observed and what is expected. Attention to phishing indicators is a necessary but not sufficient condition for detecting phishing deception. Users also need to elaborate on the indicators. During elaboration, users make conscious connections between the elements they observe and their prior knowledge [18]. The hypothesis generation, evaluation, and global assessment phases of Theory of Deception occur during the process of elaboration.

In our approach we classify an authentication ceremony regarding a specific action that a user is required to perform. The action is conveyed to the user, i.e. human node, through the communication component of the APAC Framework. The communication, conveyed through login webpages, and used in phishing attacks may contain at least some false content which could be identified during the elaboration phase.

In general, models place values on some of the variables identified as important in a framework, present relationships among the variables, and make predictions about likely outcomes. Our model makes precise assumptions about the following components of the Human Factors in APAC Framework:

Communication. The communication is an authentication ceremony login webpage. The login

page may be spoofed. We assume that the security mechanisms for detecting phishing webpages are in place, but may or may not be noticed by a user. The ceremony relies on the human to perform authentication steps bound to the login webpage and to decide whether to proceed giving their credentials; essentially deciding if the webpage is legitimate or not.

Many authentication ceremonies combine recall, recognise and compare communication. Hence, the types of communication and their combinations that our model considers are:

- Recall. Typically used in username/password authentication.
- Recognition. In a typical login procedure for recognition-based, graphical passwords systems, the user would see an image and must recognise it. Example recognition-based systems are: Passfaces [2], Dynamic Security Skins [4].
- Multiple Recognition and Recall.

Attention Maintenance. We assume that an attention switch has happened - as the user is prompted with a login page. Different authentication schemes will influence the length that attention is maintained and appropriate factors considered.

Capabilities. Knowledge of the ceremony is assumed, i.e. users knowing what credentials are expected to be sent/received to/from a server.

Motivation. Distraction from the primary task is an important factor in motivation. It can be difficult to provide as the compliant ceremony security behaviour often distracts the user from his/hers primary task.

Behaviour. Specific human behaviour that we will evaluate is as follows:

How do users process communication messages in authentication ceremonies and determine if they are genuine or not? Specifically, our model examines how users' attention to Recall and Recognise communications influences their decision-making processes and consequently their decision outcomes.

5.1. Hypothesis development

The hypotheses suggested by the Model for Analysing APAC are presented in Fig. 2 and detailed below.

The attention paid to each communication component might have a distinctly different influence on the user's likelihood to detect a fake login page. Apart from paying attention to the communication, users need to elaborate on the details, in our case on the credentials needed to be entered or evaluated. Research shows that users who elaborate on communication details are more likely to understand, learn, retain and recall the information than users who merely pay attention to them [1].

Recall requires that a user remembers information without cueing. It is generally accepted that a recall is substantially harder than recognition. Recall requires an extra cognitive effort during the elaboration phase, which otherwise may be used to notice phishing indicators.

Human ability for recognition far exceeds that for recall. Recognition, especially image recognition, is relatively easy for humans and it should require less cognitive effort. Hence:

H1: The level of Attention given to the *Recall* communication factor of the authentication ceremony will be *negatively* related to the level of elaboration.

H2: The level of Attention given to the *Recognise* communication factor of the authentication ceremony will be *positively* related to the level of elaboration.

A user's knowledge of the ceremony steps is considered an important factor that affects elaboration. It ties in with a user awareness and training approach for reducing a user's phishing susceptibility. Consistent with this approach, we expect increased ceremony knowledge to influence a user's phishing susceptibility indirectly, by influencing the user's ability to effectively elaborate and find anomalous or deceptive information.

H3: A knowledge of the ceremony (Capabilities) will be *positively* related to the level of elaboration.

The concept of motivation is important to understanding human information processing. We define motivation as the perceived relevance of a particular website to a user. Generally, information processing is more likely to occur when the user finds the services offered by a website sensitive to his/her needs and is thereby motivated to consciously evaluate credentials given to it. Also, the motivation to elaborate will be hampered by a need or urgency of the primary task that may need to be completed after the login to the website. Hence:

H4: Distraction from the primary task (Motivation) will be *negatively* related to the level of elaboration.

The influence of elaboration in phishing detection is supported by prior research [5],[12]. Hence, we posit that humans are more likely to fall victim to a phishing login webpage because they fail to elaborate on additional credentials, thereby failing to make connections between what they are presented with and the knowledge stored in their memory.

H5: Elaboration will be *negatively* related to the human's likelihood to make an *error* in the ceremony.

5.2. Hypotheses evaluation

Once hypotheses are generated, they need to be evaluated. We will evaluate the hypotheses by designing and performing a user study.

Methodology. We use *the hypothetico-deductive* method [14] from empirical social sciences research to test the model. The hypothetico-deductive experimental method is generic enough to be applied in the design and implementation of user related experiments for socio-technical systems (systems that depend on how

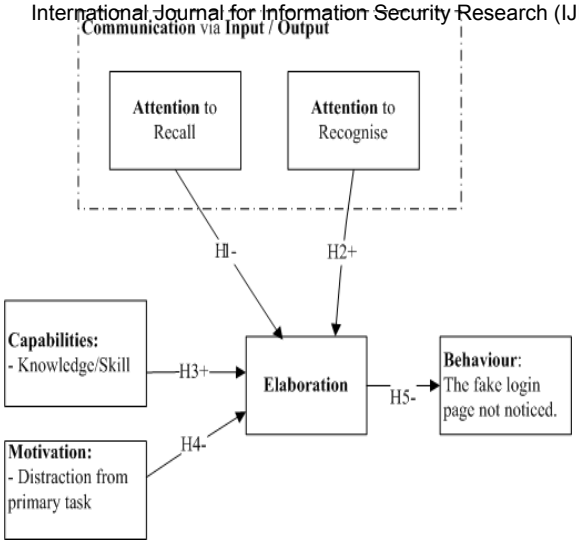

Figure 2. Model for Analysing APAC and hypotheses

humans use the technical parts). The method can be adapted to different socio-technical scenarios.

5.3. Global assessment

The last step to reach a conclusion as to whether a login webpage is deceptive consists of combining the available accepted hypotheses. The Theory of Deception [14] has emphasized that the assessment of deception can be the result of either a single strong hypothesis or the result of several weaker ones. We hypothesize that the successful users/detectors use all available hypotheses to generate an overall perception of the deceptiveness of a login webpage. We will evaluate the hypotheses by performing a user study as outlined in Section 6.

6. Evaluation of the Model for Analysing APAC

The evaluation of the Model for Analysing APAC hypotheses consists of designing and performing a user study.

6.1. Study Overview

The user study compares authentication ceremonies with regard to their impact on the user's ability to distinguish between legitimate and spoofed login web pages. Specifically, whether burdening a user with an extra authentication step makes any difference with regards to recognising a phishing login page.

Scenario. We will ask participants to imagine that they have several accounts at organizations that utilise the online login ceremonies we will introduce. We will ask them to imagine that they have the same username and password for each website. Participants will be asked to login to each of the websites and complete a set of tasks. To avoid priming, we will not inform them about the true purpose of the study. Instead, we will tell participants they are to test usability of alternative authentication schemes. Some of these websites will have altered/spoofed login pages, depending on the number of login attempts. Part of the study will be to measure if the participant noticed this or not.

Behaviour will be measured by the number of users that did/did not proceed with authentication to the fake website login page. *Elaboration* will be measured by the time the user spends when the login page appears prompting for credentials and the time he/she starts entering credentials. *Motivation* and *capabilities* will be captured via a survey that is also part of the study.

The user study is a between-subjects study where participants are randomly assigned to one of three conditions: three different authentication ceremonies. In order to compare the communication presented to the user in login pages and its effect on his/her behaviour we selected authentication schemes covering the two main communication message types and their combinations: *recall* and *recognise*. Recall and recognition are communication factors in our Human Factors in APAC Framework and the Model for Analysing APAC, as shown in Table 2 and Figure 2.

The combination of recognition and recall in the ceremonies is defined as follows:

1. *Recognition and Recall*. The user must recognise an image and then recall a text password.
2. *Multiple Recognition and One Recall*. The user must recognise multiple images and recall a text password.
3. *Multiple Recognition and Multiple Recall*. The user must recognise multiple images and recall multiple text passwords.

The user study overview is presented in Figure 3.

For each ceremony, we will implement the user interface activities for password enrolment and login according to the descriptions in the respective original papers [7], [17]. The high level design of three authentication ceremonies to be used in the study is described below.

6.2. Ceremony 1: Recognition and Recall

We have chosen Browser-Based Mutual Authentication (BBMA) [7] as a representative 'Recognition and Recall' ceremony. We already described BBMA in Section 3. For our user study we will use an image as a HPA. Hence, BBMA ceremony will involve a single object image and a text based password. In order to prove its identity to the user, the server will display the corresponding image above the login form. The user has to recognize the image and

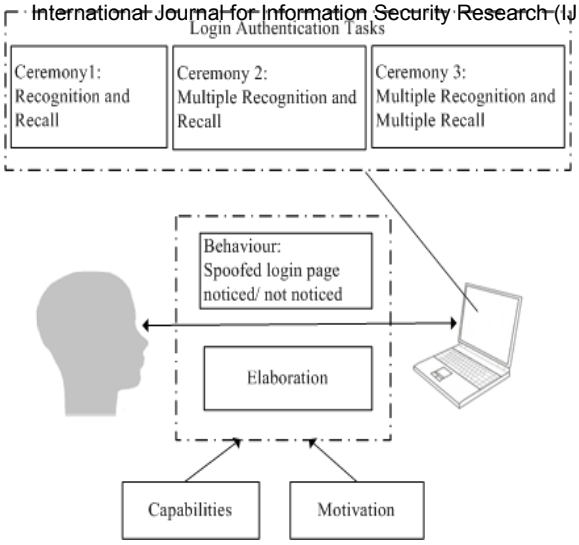

Figure 3. User study overview

then authenticate herself to the server, using a username and a text password.

6.3. Ceremony 2: Multiple Recognition and One Recall

As a representative 'Multiple Recognition and One Recall' ceremony, we will use *TwoStep: An Authentication Method Combining Text and Graphical Passwords* [17]. TwoStep is a hybrid user authentication ceremony that combines text passwords and recognition-based graphical passwords in a two-step process. In *step one*, a user is asked to supply her user name and text password. After this, even if the username/password combination is not correct, in *step two*, the user is presented with an image portfolio. The user must correctly select the images previously selected at the time of registration in each round of graphical password verification. If the selection is not correct access is denied despite a valid text password. Both the text password and all graphical passwords must be correct for the successful login.

This ceremony may be implemented in different ways according to a specific graphical password policy with regard to: number of rounds of verification; display layout; number of images to be selected in each round; an ordered or unordered image selection. We will implement it with the policy that will represent the second condition for our user study, i.e. multiple recognition and one recall: 3 rounds of verification; a 3x3 display layout; one image to be selected in each round.

6.4. Ceremony 3: MultiStep Mutual Authentication (MSMA) Ceremony

The third, 'Multiple Recognition and Multiple Recall' ceremony, is our newly proposed ceremony called *MultiStep Mutual Authentication (MSMA)*. MSMA builds on TwoStep [17] and Delayed Password Disclosure (DPD) protocols [13].

During the MSMA *registration phase* the user specifies a personal identification number (PIN), a text password and chooses a number of images. The text password is divided in parts; each part corresponds to one of the chosen images.

As part of *login phase*, a *PIN* is used in step one. In subsequent steps, a combination of a *graphical* and a *text* password is used.

The user enters the text password in parts: each part consists of a number of characters/digits. To *enable entry* for a part of the text password, the user must first select an image from the presented image set. The image sets are presented sequentially after the user enters his username and PIN and provide visual authenticity feedback. If the user is presented with an image set that does not contain the right image, they should stop entering the text password to avoid disclosing all parts to a fake website. The attacker (i.e. phisher) would have difficulties to present image sets with the images selected at the time of registration. If either the username, the PIN or the image selected by the user in a previous step is incorrect, the presented image set will not contain the corresponding image.

All authentication credentials: the PIN, the set of images and the text password must be correct for a successful login.

MSMA can be adapted to have fewer or more steps, depending in how many parts is the text password divided. Also, the size of the parts that the password is divided into can vary, e.g to be just one character or digit.

For our user study we will divide a text password in *three parts*: each part consisting of one character/digit and corresponding to *one image* from a graphical feedback password. A 3x3 display layout will be used for presenting the image set containing the corresponding image and other random images.

MSMA user login steps will then be as follows:

- *Step 1*: The user enters username and PIN.
- *Step 2*: The first set of images is presented to the user.

  The user clicks on the recognised image and then enters the 1st part of the text password.
- *Step 3*: The second set of images is presented to the user.

  The user clicks on the recognised image and then enters the 2nd part of the text password.
- *Step 4*: The third set of images is presented to the user.

  The user clicks on the recognised image and then enters the 3rd part of the text password.
- *Step 5*: The user submits the text password, that is concatenated from the three parts.

7. Conclusions and Future Work

We proposed a Human Factors in Anti-Phishing Authentication Ceremonies (APAC) Framework for investigating human-protocol interaction factors affecting phishing attacks success in authentication ceremonies. We showed how to apply the framework to model human-protocol behaviour. The resulting Model for Analysing APAC correlates the human node decisions making factors in authentication ceremonies. We also outlined how to evaluate the model with a user study and proposed an initial design of MultiStep Mutual Authentication (MSMA), an anti-phishing authentication ceremony. The user study compares authentication ceremonies with regard to their impact on the user's ability to distinguish between legitimate and spoofed login web pages.

Future work includes performing the user study and analysing the data. The results of the study will be used to improve design of MSMA ceremony.

8. References

[1] R. Cialdini. *Influence: Science and Practice*. Pearson Education, Inc., 5th edition, 2009.

[2] R. U. Corporation. The science behind passfaces. Technical report, Real User Corporation, June 2004.

[3] L. F. Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, Berkeley, CA, USA, 2008. USENIX Association.

[4] R. Dhamija and D. Tygar. The battle against phishing: Dynamic security skins. In *Symposium on Usable Privacy and Security (SOUPS) 2005*, Pittsburgh, PA, USA, July 2005. ACM.

[5] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In *CHI Conference on Human Factors in Computing Systems*, Montreal, Quibec, Canada, April 2006.

[6] C. Ellison. Ceremony design and analysis. Technical Report 2007/399, Carnegie Mellon University, 2007.

[7] S. Gajek, M. Manulis, A. Sadeghi, and J. Schwenk. Provably secure browser-based user-aware mutual authentication over tls. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pages 300–311. ACM, March 2008.

[8] A.-P. W. Group. Phishing activity trends report, 3rd quarter 2014. Technical report, Anti-Phishing Working Group, March 2015.

[9] M. Hart, C. Castille, M. Harpalani, J. Toohill, and R. Johnson. Phorcefield: A phish-proof password ceremony. In *The 27th Annual Computer Security Applications Conference (ACSAC 2011)*, Orlando, Florida, USA, December 2011.

[10] E. Hatunic-Webster, F. Mtenzi, and B. O'Shea. Poster: Towards a model for analysing anti-phishing authentication ceremonies. In *Symposium on Usable Privacy and Security(SOUPS)*, Newcastle, UK, July 2013.

[11] E. Hatunic-Webster, F. Mtenzi, and B. O'Shea. Model for analysing anti-phishing authentication ceremonies. In *Proceedings of 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, London, UK, December 2014. IEEE.

[12] M. Jakobsson. The human factor in phishing. In *Privacy and Security of Consumer Information '07*, 2007.

[13] M. Jakobsson and S. Myers. Delayed password disclosure. *Int. J. Applied Cryptography*, 1(1):47–59, 2008.

[14] P. Johnson, S. Grazioli, K. Jamal, and I. I.A. Zualkernan. Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes*, 53(2):173–203, 1992.

[15] C. Karlof, J. Tygar, and D. Wagner. Conditioned-safe ceremonies and a user study of an application to web authentication. In *The 5th Symposium on Usable Privacy and Security, SOUPS '09*, Mountain View, CA, USA, July 2009.

[16] K. Radke, C. Boyd, J. Nieto, and M. Brereton. Towards a secure human-and-computer mutual authentication protocol. In *Australasian Information Security Conference (AISC) 2012*, RMIT University, Melbourne, Australia, 30 Jan - 3 Feb 2012.

[17] P. van Oorschot and T. Wan. Twostep: An authentication method combining text and graphical passwords. In *4th MCETECH Conference on eTechnologies*, May 2009.

[18] A. Vishwanath, T. Herath, R. Chen, J. Wang, , and H. Rao. Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51:576–586, 2011.

[19] J. Wang, H. Tejaswini, R. Chen, A. Vishwanath, and H. Rao. Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4):345–362, 2012.

[20] M. Wogalter, D. Dejoy, and K. Laughery. *Warnings and Risk Communication*. Taylor and Francis, Philadelphia, PA., 1999.