Poster: Towards a Model for Analysing Anti-Phishing Authentication Ceremonies

Edina Hatunic-Webster
Dublin Institute of Technology
Dublin, Ireland
edina.hatunic-webster@dit.ie

Fred Mtenzi
Dublin Institute of Technology
Dublin, Ireland
fredrick.mtenzi@dit.ie

Brendan O'Shea
Dublin Institute of Technology
Dublin, Ireland
brendan.oshea@dit.ie

1. INTRODUCTION

Phishing uses both social engineering and technical means to carry out attacks. Therefore, human factors - incorrect human trust decisions play an important role in phishing. Many online authentication techniques place a disproportional burden on human abilities. Assumptions made about human-protocol behaviour are often flawed.

In our approach we use the concept of a ceremony to analyse and improve the anti-phishing security of web authentication.

A ceremony [4] is an extension of the concept of network protocol that includes user interface, human-to-human communication and transfers of physical objects that carry data. It is one way of extending the reach of current methods for analysing protocols to include humans. A secure ceremony is secure against both normal and social engineering attacks, such as phishing.

The complexity of defining a ceremony comes with modelling a human node and 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 [4], [1].

In this paper we present our recent and on-going work on researching human communication processing in anti-phishing authentication ceremonies. We propose a new Human Factors in Anti-Phishing Authentication Ceremonies (APAC) framework and outline how to apply the framework to model human node behaviour. By applying our model, it will be possible to identify design principles for minimising human node interaction errors in anti-phishing authentication ceremonies.

2. APAC FRAMEWORK

The Human Factors in APAC Framework is based on a communication processing model in which a communication is sent to a user, triggering some behaviour, as shown in Figure 1. The framework builds on Cranor's [2] Human-in-the-Loop Security Framework, which is an established framework for evaluating secure systems. 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.

Different to Cranor, we aim to provide a more specific model of human information processing, that correlates the components of the APAC framework.

Table 1 gives an overview of the components of our APAC framework and the factors that impact the anti-phishing security of authentication ceremonies. The framework components were determined by reviewing existing anti-phishing authentication techniques according to anti-phishing security characteristics and user-interaction features. A brief description of the components is given below.

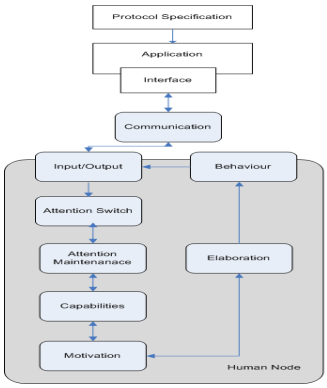

Figure 1: Human Factors in APAC Framework

Communication. We distinguish three types of communications to the human node: *recognise*, *recall* and *compare*. There are specific issues that may arise from each.

Input and Output. The type of input affects the level of user's acceptance of the ceremony and hence the anti-phishing security.

Attention Switch. Ceremony security analysis needs to make sure that the human node has indeed received the intended communication. Factors to consider are: *colour*, *font*, *size*, *motion* and *sound*.

Attention Maintenance. This component is vulnerable to *habituation*, the tendency for users to pay less attention to stimuli they experience frequently [2]. Another common behaviour is the user who skips a security step, as he is *rushing* to finish a primary task (provided by a service provider).

Capabilities. An important aspect of an authentication ceremony is how newly created authentication credentials are remembered and later retrieved at login. We distinguish two types of capabilities that affect this process: *memory* and *comprehension*.

Motivation. Motivation plays an important role in how users decide what action they are willing to take. Users often do not believe that they will be a target of a phishing attack. Hence: *risk perception*, *distraction from primary task*, *convenience*, *rushing user* and *incentives/disincentives* are the types of motivation to be considered.

Table 1: The Components of the APAC Framework

Component	Factors to Consider
Communication	Recognise, Recall, Compare
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	Skip a required step Predictable Perform an action incorrectly

Elaboration. Elaboration is the process by which users make conscious connections between the cues they observe and previous knowledge[6]. The importance of elaboration in deception detection is supported by prior phishing research[3].

Behaviour. Users make three types of behavioural errors: mistakes, lapses or slips. These may result in a protocol step not achieving the desired goal; users skipping a required step or performing an action incorrectly. The predictability of behaviour may also be exploited by phishers[2].

We intend to validate the framework and correlate its components by designing a new *Model for Analysing APAC*.

3. MODEL FOR ANALYSING APAC

The main purpose of our Model for Analysing APAC is to test a specific part of the APAC framework and determine the *likelihood of a user making an error*, hence increasing the probability of phishing attacks success. The aim is to determine the importance of each factor involved in the decision making by a human node in an authentication ceremony.

The model is grounded in the prior research in information processing and decision making [6], [5]. The decision-making process in the model incorporates concepts of Vishwanath's [6] Information Processing Model of Phishing Susceptibility, which has its root in the Theory of Deception [5]. As phishers apply deception to fool the user to give away authentication credentials, it seems a plausible approach to model human node decision-making. We intend to test the model by conducting a survey and using the hypothetico-deductive method of reasoning [5]. The first draft of the model and hypotheses defined is presented in Figure 2.

The hypotheses, as *currently* defined are:

- **H1.** The level of attention given to specific elements of the authentication ceremony will be negatively related to the level of elaboration.
- **H2.** Elaboration will be negatively related to the human node's likelihood to make an error in the ceremony.

The model will be further refined, the rest of the hypotheses defined and more precise assumptions about the components will be made: e.g. attention switch to the expected ceremony; attention maintenance to authentication factor *n*.

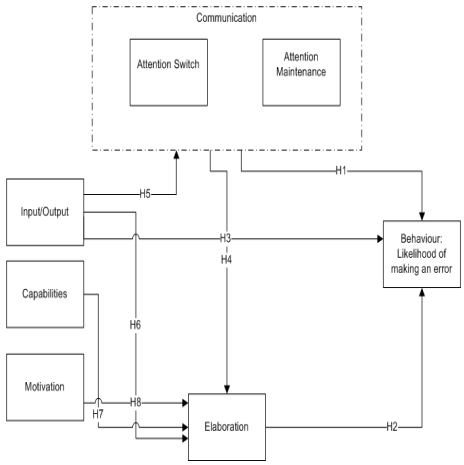

Figure 2: Model for Analysing APAC

4. CONCLUSIONS

In our approach we use the concept of a ceremony to analyse and improve the anti-phishing security of web authentication. We propose a Human Factors in Anti-Phishing Authentication Ceremonies (APAC) framework in order to model the communication processing performed by human nodes. We have started the design of a model whose main purpose is to evaluate and correlate the framework components and identify principles for minimising human node interaction errors in anti-phishing authentication ceremonies. Future work includes applying these principles to propose a new phishing resistant authentication ceremony. Importantly, user study results of the APAC designed in this way can be compared with theoretical premises set by the framework and the model.

5. REFERENCES

[1] M. C. Carlos and G. Price. Understanding the weaknesses of human-protocol interaction. In *Workshop on Usable Security at 16th International Conference on Financial Cryptography and Data Security*, March 2012.

[2] L. F. Cranor. A framework for reasoning about the human in the loop. Technical Report CMU-CyLab-08-001, Carnegie Mellon University, 2008.

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

[4] C. Ellison. Ceremony design and analysis. Technical Report 2007/399, Cryptology ePrint Archive, 2007.

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

[6] 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.