Perception of Risky Security Behaviour by Users: Survey of Current Approaches

Lynsay A. Shepherd, Jacqueline Archibald, and R.I. Ferguson

University of Abertay Dundee, School of Engineering, Computing and Applied Mathematics, Dundee, DD1 1HG
{lynsay.shepherd,j.archibald,i.ferguson}@abertay.ac.uk

Abstract. What constitutes risky security behaviour is not necessarily obvious to users and as a consequence end-user devices could be vulnerable to compromise. This paper seeks to lay the groundwork for a project to provide instant warning via automatic recognition of risky behaviour. It examines three aspects of the problem, behaviour taxonomy, techniques for its monitoring and recognition and means of giving appropriate feedback. Consideration is given to a way of quantifying the perception of risk a user may have. An ongoing project is described in which the three aspects are being combined in an attempt to better educate users to the risks and consequences of poor security behaviour. The paper concludes that affective feedback may be an appropriate method for interacting with users in a browser-based environment.

Keywords: End-user security behaviours, usable security, affective computing, user monitoring techniques, user feedback, risk perception, security awareness.

1 Introduction

Despite the widespread availability of security tools such as virus scanners and firewalls, risky behaviour exhibited by the end-user has the potential to make devices vulnerable to compromise [1]. This paper aims to identify what constitutes risky security behaviour, review current methods of monitoring user behaviour, and examine ways in which feedback can be provided to users with a view to educating them into modifying their behaviour when browsing the web. Previous work has indicated users need to learn and recognise patterns of risky behaviour themselves [21] [22], thus improving system security.

2 Background

Users often regard system security as obtrusive and restrictive of their ability to perform tasks. Owing to this, they often attempt to circumvent these measures, at the risk of breaching system security [2]. It is possible to place risky security behaviours into categories, allowing monitoring techniques to be developed which attempt to capture the behaviour.

L. Marinos and I. Askoxylakis (Eds.): HAS/HCII 2013, LNCS 8030, pp. 176–185, 2013.

2.1 Types of Behaviour

There are a number of ways in which user behaviour could be perceived as risky e.g. interaction with poorly constructed web-based applications may place users at risk from coding vulnerabilities [11]. Other risky behaviours include creating weak passwords, sharing passwords [3] [12] and downloading data from unsafe websites [13].

The problem can be exacerbated by misplaced trust in a comfortable computing environment: if a user interacts with a device regularly, they may form a knowledge-based trust relationship with it [24] (as cited in [25]) whereby, based upon their history with the device, they become accustomed to its peculiarities. Such familiarity may cause the user to be over trustful of interactions performed on it. Knowledge-based trust is said to be persistent and even if performance differs, the trust relationship remains.

2.2 Monitoring Techniques/Measuring Awareness

It is possible that risky security behaviour can be automatically recognised through user monitoring. Previous studies [4] [5] refer to the use of an event-based system, allowing user's actions to be monitored across a range of applications running on the operating system. Video monitoring is also a technique which has been used successfully. In particular, it has been used to record eye movements of users, thus determining the affective state of the end-user [6]. When used in combination with a task-based approach, video monitoring can provide a detailed overview of end-user behaviour, in comparison to approaches monitoring a singular type of interaction [7].

Monitoring techniques are just one component which can be investigated when exploring the issue of end-user security behavior. When measuring awareness it is useful to record the perception of risk which users have. Several pieces of research have been conducted in the area, investigating suitable metrics for describing the perception of risk. Previous studies have employed questionnaires to assess how the user perceives their behavior [8]. This concept can be extended to make use of both questionnaires and psychometric models, providing an overview of perceived risky behaviour [14] [15].

2.3 Types of Feedback

There are many methods of providing user feedback. These include pieces of textual information, where specific words are used e.g. describing a password as "weak" [9]. Colour can be used in combination with text, or alone in a bar meter, displaying either green/blue to imply "good" or red for "bad" [9]. Furthermore, dialogue, colours and sounds can be used together to alter the affective state of a user [18].

Avatars have been widely implemented to change the affective state of the user, particularly in the field of intelligent tutoring agents. In a number of instances the

introduction of avatars has proved beneficial and has helped users in educational environments [18] [19] [20].

3 Analysis

This section explores previous research, to provide a comparison of terminology used when describing risky security behaviour. Applying monitoring techniques to users can capture such behaviour and allow perception of risk to be measured. Potentially, user behaviour could be influenced by feedback provided.

3.1 Risky Behaviour – A Taxonomy

There have been several attempts to categorise behaviours displayed by users which could be classified as risky (summarised in Table 1), including a 2005 paper by Stanton et al. [3]. Following interviews with both security experts and IT experts, and a study involving end-users in the US, across a range of professions, a taxonomy of 6 behaviours was created: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance and basic hygiene.

Padayachee [26] provides a breakdown of compliant security behaviours whilst investigating if certain users had a predisposition to adhering to security behaviour. A taxonomy was developed, highlighting elements which may influence security behaviours in users i.e. extrinsic motivation, identification, awareness and organisational commitment. The paper acknowledges the taxonomy does not present a complete overview of all possible motivational factors regarding compliance with security policies. Despite this, it may provide a basis as to how companies could start to improve their security education, with a view to gaining the attention of end-users.

In terms of common risky behaviours, passwords can be problematic with a trade-off existing between the usability of passwords and the level of security they provide [12]. Usable passwords are easier for users to remember however, this can mean they are short and therefore less secure. Users may also engage in questionable behaviour e.g. sharing passwords. Whilst exploring the issue of basic security hygiene, Stanton et al. [3] touched on the subject of passwords. A survey of 1167 end-users highlighted several instances of risky security behaviour e.g. 27.9% of participants wrote their passwords down and 23% revealed their passwords to colleagues.

Another of these categories is related to how users perceive technology flaws, e.g. vulnerability to XSS attacks or session hijacking. Social engineering can also be considered to fall into this category: e.g. An attacker could potentially clone a profile on a social networking site and use the information to engineer an attack against a target(eg via the malicious link technique) [11]. Such attacks can be facilitated by revealing too much personal information on social networking sites [10].

Downloading illegal files such as music/software can be classed as risky behaviour: in addition to breaking the law, users are potentially exposing their system to viruses or malware that the downloaded files may contain [13].

Table 1. - Comparison of terminology describing risky security behaviours

[3] Stanton, J.M. et al.	[26] Padayachee, K.	[12] Payne, B. and Edwards, W	[10] Balduzzi, M.	[11] Hadnagy, C.	[13] Fetscherin, M.	[29] Herath, T. and Rao, H.R.
Intentional destruction: intention to harm IT resources in a company	Amotivation	-	-	-	-	-
Detrimental misuse: using IT for inappropriate purposes	Amotivation	-	-	-	Download-ing illegal files	-
Dangerous tinkering: accidentally configuring IT resources with security flaws	-	-	-	-	-	-
Naïve mistakes: user doesn't realise their behaviour is flawed	-	Password usability	Sharing too much on social networks	Sharing too much on social networks	-	-
Aware assurance: wants to protect company IT systems- recognises security issues.	Extrinsic motivation	-	-	-	-	Intrinsic motivation: perceived effectiveness
Basic hygiene: user is educated about security issues and adheres to security policies	Extrinsic and intrinsic motivation	Password usability	-	-	-	Extrinsic motivation :social pressures

3.2 Monitoring Risky Behaviour

Multiple approaches have been used in the past to monitor user behavior. Fenstermacher and Ginsburg [5] have experimented with the use of a system event-based approach (originally designed for gathering usability information) which linked applications running across the operating system. Each application invoked several method calls and functions, making use of Microsoft's Component Object Model and Python. An XML-based log file was then generated based-upon the actions of the user, containing information such as a timestamp, the application used and which event was triggered. This suggests a similar technique could be applied when monitoring risky security behaviour.

Additionally, a combination of video and task monitoring could be used to view user behavior [6]. In a study by Heishman, the eye movement of participants was monitored to interpret the affective state of the user. Results of the study found it was

possible to detect the affective and cognitive states of users and that such a technique may be used when exploring further HCI concepts.

Doubleday et al. also successfully used both video and task monitoring to observe behavior [7]. In this study, users were given a series of tasks to complete e.g. retrieving information from a database. Whilst completing the assigned tasks, users were asked to provide a running commentary of their thoughts. They were observed via a video camera during this process to gauge their level of interaction with the system. Additionally, they were provided with a questionnaire on completion, comprising of a 7-point Likert scale regarding usability aspects of the system e.g. the appeal of the system used. The research highlights that when monitoring risky behaviour, a multimodal approach is useful, allowing a comparison of results from each monitoring method.

3.3 Measuring Perception of Risk

It can be hard for the user to recognise their security behaviour as risky. A number of techniques have been used to gauge the perception of risk (summarised in Table 2). Farahmand et al. [14] explored the possibility of using a psychometric model originally developed by Fischoff et al. [15] in conjunction with questionnaires, allowing a user to reflect on their actions and gauge their perception, providing a qualitative overview.

Takemura [27] also used questionnaires when investigating factors determining the likelihood of workers complying with information security policies defined within a company, in an attempt to measure perception of risk. Participants were asked a hypothetical question regarding whether or not they would implement an anti-virus solution on their computer if the risk of them getting a virus was 10%, 20% and etc. Results revealed that 52.7% of users would implement an antivirus solution if the risk was only 1% however, 3% of respondents still refused to implement antivirus, even when the risk was at 99% which displays a wide range of attitudes towards risk perception. The study concluded that risk perception was a psychological factor with the potential to influence problematic behaviours.

San-José and Rodriguez [28] used a multimodal approach to measure perception of risk. In a study of over 3000 households with PCs connected to the internet, users were given an antivirus program to install which scanned the machines on a monthly basis. The software was supplemented by quarterly questionnaires, allowing levels of perception to be measured and compared with virus scan results. Users were successfully monitored and results showed that the antivirus software created a false sense of security and that users were unaware of how serious certain risks could be.

Ng, Kankanhalli and Xu [16] examined the use of a health belief analogy when explaining the perception of risk in terms of cyber security. The perception of falling ill was directly related to a) the perceived susceptibility of falling ill and b) how severe the illness is perceived to be. When translated to the field of cyber security, it was discovered these factors along with perceived benefits, perceived barriers, cues to action, general security orientation and self-efficacy can help to determine the riskiness of user behaviour. Experiments were conducted with an example based upon email attachments. It was concluded that users security behaviour could be determined via perceived susceptibility, perceived benefits, and self-efficacy.

Table 2. - Comparison of methods used for measuring perception of risky behaviour

Technique	Description
Psychometric model	Used the models to determine characteristics relating to gauging perception of security and privacy risks [14].
Questionnaires	Subjects were assigned questionnaires to allow them to reflect on their perception of risk [14].
	Used to determine the likelihood of workers complying with information security policies [27].
	Used quarterly questionnaires to gauge perception of risk. Compared these to anti-virus scan results [28].
Technology-based	Installed antivirus software on over 3000 internet connected PCs which were scanned on a monthly basis [28].
Health belief model	The model was used as an analogy to explain perception of risk [16].

3.4 Feedback

Several methods can be deployed to inform the user that they are exhibiting risky behaviour (summarised in Table 3). Ur et al. [9] investigated ways in which feedback could be given to users, in the context of aiding a user in choosing a more secure password. Research conducted found that users could be influenced into increasing their password security if terms such as "weak" were used to describe their current attempt. In the research, colour was also used as a factor to provide feedback to users. When test subjects were entering passwords into the system, a bar meter was shown next to the input field. Depending upon the complexity of the password, the meter displayed a scale ranging from green/blue for a good/strong password to red, for a simplistic, easy to crack password. Data gathered from the experiments showed that the meters also had an effect on users, prompting them to increase system security by implementing stronger passwords.

Multimedia content such as the use of colour and sound [18] can also be used to provide feedback to the user. In a game named "Brainchild" developed by McDarby et al., users must gain control over their bio-signals by relaxing. In an attempt to help users relax, an affective feedback mechanism has been implemented whereby the sounds, colours and dialogues used provides a calming mechanism.

Textual information provided via the GUI can be used to communicate feedback to the user [17]. Dehn and Van Mulken conducted an empirical review of ways in which animated agents could interact with users. In doing so, they provided a comparison between the role of avatars and textual information in human-computer interaction. It was hypothesised that textual information provided more direct feedback to users however, avatars could be used to provide more subtle pieces of information via gestures or eye contact. Ultimately it was noted multimodal interaction could provide users with a greater level of communication with the computer system.

Previous research has indicated that affective feedback can be utilised when aiding users in considering their security behaviour online, since it can detect and help users

alter their internal states [18]. Work conducted by Robison et al. [19] used avatars in an intelligent tutoring system to provide support to users, noting that such agents have to decide whether to intervene when a user is working, to provide affective feedback. However, there is the danger that agents may intervene at the wrong time and in doing so, may cause some negative affects when attempting to aid a student.

Hall et al. [20] concurs with the notion of using avatars to provide affective feedback to users, indicating that they influence the emotional state of the end-user. Avatars were deployed in a personal social and health education environment, to educate children about the subject of bullying. Studies showed that the avatars produced an empathetic effect in children, indicating that the same type of feedback could be used to achieve the same result in adults.

Table 3. - Comparison of feedback techniques

Technique	Description
Textual	Specific words were chosen to persuade participants to consider password security i.e. participants would not want a password to be described as "weak" [9].
	Textual data can provide more direct feedback [17].
Colour	Used colours in bar meters to indicate password strength [9].
	Specific colours used to allow users to control their state [18].
Sound	Specific music used to allow users to control their state i.e. calming music [18].
Avatars	General overview of the role of animated agents in HCI [17].
	Avatars were utilised in an intelligent tutoring system, to support users learning about microbiology and genetics [19].
	Avatars were deployed in a personal social and health environment to provide education on bullying [20].

4 Conclusion/Future Work

It has been observed that educating users about security issues is key to reducing risky behaviour however this is notoriously difficult [21] [22]. Ng, Kankanhalli and Xu concur with this sentiment [16], specifically stating that users should be trained about various security controls, and what they are used for, therefore improving the user's understanding and level of self-efficacy. Ultimately, this will improve system security.

Work currently being undertaken by Shepherd [23] seeks to advance the field by exploring the role of affective feedback in enhancing security risk awareness, focussing on a browser-based environment. Previous research has indicated that affective computing may serve as a method of educating users about risky security behaviours. The project seeks to develop an initial software prototype (in the form of a Firefox extension) to monitor user interaction within a web browser, comparing captured behaviour to models of known risky behaviours. The prototype will then be developed further, with the addition of feedback agents, featuring affective feedback techniques in an attempt to investigate a) if security risk awareness improves in end-users and b) if system security improves through the use of affective feedback.

References

1. Li, Y., Siponen, M.: A call for research on home users information security behaviour. In: PACIS 2011, Proceedings (2011) (paper 112)
2. Pfleeger, S., Caputo, D.: Leveraging behavioral science to mitigate cyber security risk, Computers & Security (2012), doi:10.1016/j.cose.2011.12.010 (accessed October 29, 2012)
3. Stanton, J.M., et al.: Analysis of end user security behaviors. Computers and Security 24, 124–133 (2005)
4. Hilbert, D., Redmiles, D.F.: Extracting usability information from user interface events. ACM Computing Surveys, 384–421 (December 2000)
5. Fenstermacher, K.D., Ginsburg, M.A.: Lightweight framework for cross-application user monitoring. IEEE Computer, 51–58 (2002)
6. Heishman, R., Duric, Z., Wechsler, H.: Understanding cognitive and affective states using eyelid movements. In: First IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS 2007, September 27-29, pp. 1–6 (2007), http://dx.doi.org/10.1109/BTAS.2007.4401944 (accessed November 2, 2012)
7. Doubleday, A., et al.: A comparison of usability techniques for evaluating design. In: Coles, S. (ed.) Proceedings of the 2nd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, DIS 1997, pp. 101–110. ACM, New York (1997), http://doi.acm.org/10.1145/263552.263583 (accessed November 2, 2012)
8. Staddon, J., et al.: Are privacy concerns a turn-off?: engagement and privacy in social networks. In: Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS 2012, Article 10, 13 pages. ACM, New York (2012), http://doi.acm.org/10.1145/2335356.2335370 (accessed November 2, 2012)
9. Ur, B., et al.: How does your password measure up? The effect of strength meters on password creation. In: Security 2012 Proceedings of the 21st USENIX Conference on Security Symposium, Berkeley, CA, USA (2012); Also presented at Symposium On Usable Privacy and Security, July 11-13, pp. 462–469. ACM, Washington, DC (2012), https://www.usenix.org/conference/usenixsecurity12/how-does-your-password-measure-effect-strength-meters-password-creation (accessed November 2, 2012)
10. Balduzzi, M.: Attacking the privacy of social network users. HITB Secconf 2011 Malaysia (2011), http://conference.hitb.org/hitbsecconf2011kul/materials/D1T1%20%20Marco%20Balduzzi%20-%20Attacking%20the%20Privacy%20of%20Social%20Network%20Users.pdf (accessed September 21, 2012)
11. Hadnagy, C.: Social engineering: the art of human hacking, pp. 23–24. Wiley Publishing, Indianapolis (2011)
12. Payne, B., Edwards, W.: A brief introduction to usable security, pp. 13–21 (May/June 2008)
13. Fetscherin, M.: Importance of cultural and risk aspects in music piracy: A cross-national comparison among university students. Journal of Electronic Commerce Research (January 2009), http://www.csulb.edu/journals/jecr/issues/20091/Paper4.pdf (accessed October 30, 2012)

14. Farahmand, F., et al.: Risk perceptions of information security: A measurement study. In: Proceedings of the 2009 International Conference on Computational Science and Engineering, CSE 2009, vol. 3, pp. 462–469. IEEE, Washington, DC (2012), http://dx.doi.org/10.1109/CSE.2009.449 (accessed November 2, 2012)
15. Fischoff, B., et al.: How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sciences 9(2), 127–152 (1978)
16. Ng, B., Kankanhalli, A., Xu, Y.: Studying users' computer security behavior: A health belief perspective. Decision Support Systems 46(4), 815–825 (2009), http://dx.doi.org/10.1016/j.dss.2008.11.010, doi:10.1016/j.dss.2008.11.010 (accessed December 6, 2012)
17. Dehn, D., Van Mulken, S.: The impact of animated interface agents: a review of empirical research. International Journal of Human– Computer Studies 52(1), 1–22 (2012), http://dx.doi.org/10.1006/ijhc.1999.0325 (accessed May 30, 2012)
18. McDarby, G., et al.: Affective feedback. Media Lab Europe (2004), http://medialabeurope.org/mindgames/publications/publicationsAffectiveFeedbackEnablingTechnologies.pdf (accessed May 22, 2012)
19. Robison, J., McQuiggan, S., Lester, J.: Evaluating the consequences of affective feedback in intelligent tutoring systems. In: Proceedings of International Conference on Affective Computing and Intelligent Interaction, ACII 2009, Amsterdam, pp. 37–42. IEEE (2009), http://www4.ncsu.edu/~jlrobiso/papers/acii2009.pdf (accessed May 22, 2012)
20. Hall, L., Woods, S., Aylett, R.S., Newall, L., Paiva, A.C.R.: Achieving empathic engagement through affective interaction with synthetic characters. In: Tao, J., Tan, T., Picard, R.W. (eds.) ACII 2005. LNCS, vol. 3784, pp. 731–738. Springer, Heidelberg (2005)
21. Jakobsson, M., Ramzan, Z.: Crimeware: understanding new attacks and defenses, p. 400. Addison-Wesley, Upper Saddle River (2008)
22. Ed Team. Social. HITB Magazine 1(6), 44–47 (2011), http://magazine.hitb.org/issues/HITB-Ezine-Issue-006.pdf (accessed September 21, 2012)
23. Shepherd, L.: Enhancing security risk awareness in end-users via affective feedback. PhD Proposal, University of Abertay, Dundee (2012) (unpublished)
24. Lewicki, R.J., Bunker, B.B.: Developing and maintaining trust in work relationships. In: Kramer, R., Tyler, T. (eds.) Trust in Organizations: Frontiers of Theory and Research, pp. 114–139. Sage Publications, Thousand Oaks (1996)
25. Mcknight, D., et al.: Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems 2(2), Article 12 (2012), http://dx.doi.org/10.1145/1985347.1985353 (accessed December 6, 2012)
26. Padayachee, K.: Taxonomy of compliant information security behavior. Computers & Security 31(5), 673–680 (2012), http://dx.doi.org/10.1016/j.cose.2012.04.004 (accessed December 6, 2012)
27. Takemura, T.: Empirical analysis of behavior on information security. In: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ITHINGSCPSCOM 2011, pp. 358–363. IEEE Computer Society, Washington, DC (2011), http://dx.doi.org/10.1109/iThings/CPSCom.2011.8 (accessed January 7, 2013)

28. San-José, P., Rodriguez, S.: Study on information security and e-Trust in Spanish households. In: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2011, pp. 1–6. ACM, New York (2011), http://doi.acm.org/10.1145/1978672.1978673 (accessed January 7, 2013)
29. Herath, T., Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Syst. 47(2), 154–165 (2009), http://dx.doi.org/10.1016/j.dss.2009.02.005 (accessed January 31, 2013)