A Study on Improving Security Warnings

Zarul Fitri Zaaba[1,2], Steven M. Furnell[2,3] and Paul S. Dowland[2]
[1]School of Computer Sciences,
Universiti Sains Malaysia, Penang, Malaysia
[2]Centre for Security, Communications and Network Research,
Plymouth University, United Kingdom
[3]Security Research Institute Edith Cowan
University Perth, Western Australia
zarulfitri@cs.usm.my, info@cscan.org

Abstract – **Security warnings are intended to alert users about the possibility of events that may compromise their protection. They encounter security warnings on daily basis in many situations when dealing with their computer. However, prior studies have shown that users often have difficulty in understanding the warnings, which can pose a particular risk in cases where they are required to make a decision. Well gathered information is needed to help the researchers and other people to further understand this area. This paper describes an overview of studies on security warnings. It covers problems that end users encounter with security warnings, possible solutions and approaches of security warnings and useful classification of security warnings studies. It is expected that this paper will benefit the research community or general public to understand the problems and possible solutions in improving security warnings.**

Keywords – Security, Warning, Interface, Usability, Usable security

I. INTRODUCTION

In view of increasing threats in computer usage, today's users need to be familiar with the use of security tools and how to interact with related system functionality. However, in many cases a major challenge is about the usability of the technologies because users can face difficulties in understanding them correctly and utilizing them effectively. One area that needs focus is the issue of interaction with these tools, particularly when users are presented with a warning to inform or to remind them that something untoward is happening or is going to happen.

It is not at all uncommon for users to encounter warnings in which they are presented with more than one option and there are no specific features to support them in making a decision. Often, the decision that they have to make may have significant consequences (i.e. users do not realise the impact of the decision on the security and protection of the computer). Therefore, this could jeopardize the fundamental goal of computer security (i.e. confidentiality, integrity and availability). This paper provides an overview of security warnings studies based on a review of user interactions with security tools and technologies.

II. RELATED WORKS

Warnings can be defined as safety communications that are used to inform people about hazards to protect them from any harm [1]. Warnings can also be defined as anything that can alert an individual's attention towards potentially dangerous circumstances [2]. Therefore, in general a warning is a method to inform about the occurrence of risks or problems in the future and it can help to protect the users from harm. A similar concept can be applied to computer warnings, as all applications (e.g. web browsers) inform users using warnings representation based on its contexts and the level of severity (e.g. dialogue box, balloons, banners, and notifications).

As a medium of communication to inform users about possible issues in computer systems, warning functions must be presentable. A user should be able to comprehend the current problems they are facing and later be guided to make better decisions. Many observations and user studies have looked at various domains such as virus alerts and active browser warnings [3], online banking context [4] and privacy and policy [5]. Microsoft had taken steps to improve previous warning dialogues (i.e. defaults buttons, labels, primary text, footnote area and assistance text) [6].

Based on our investigation, many issues have been raised in relation to security warnings. However, not much focus has been given on classification approaches to improve security warnings and its architecture. This paper intends to provide some useful information to clarify these issues.

The outline of this paper is as follows: section 2 will explain an overview of issues in security warning studies such as the problems, solutions and approaches. Section 3 highlights discussions on relevant issues, Section 4 explains the future works and finally, section 5 provides the conclusions.

A. *Investigation on security warnings problems*

Security warnings in computer context can be classified to five different types shown in Table I [7]. Each user interface contexts works with a specified situation and Microsoft already had their own standard to implement it. Microsoft had been chosen due to its popularity and widely used by end users.

TABLE I. 5: DIFFERENT USER INTERFACE CONTEXTS

User Interface Contexts	Suitable Usage
Dialogue Box	Used for critical warnings that includes confirmation. Users must respond to the warning instantly (Modal dialogue box)
In-Place	Used to provide information that possibly prevents a problem. It is useful when users are making choices
Notifications	Used with significant circumstances or status that can be safely ignored by users (at least temporary)
Balloons	Used as a control in a situation that affects the input. This state is likely to be unintended and users may not realize that the input is affected.
Banners	Used to provide information that may prevent a problem. It is useful for users in completing a task

Although there is a standard that has been used, end-users are still baffled by security warnings that they encounter on a daily basis. For instance, a user study with 30 participants conducted to prevent phishing attacks the results show that participants ignore the warning especially when the web content looked legitimate [8].

On the other hand, a web based survey involving 114 users was conducted to evaluate the effectiveness of security warnings in a web browser setting [9]. The results revealed that users still ignore the warning as it did not convince them to make a better action. In addition, respondents claimed the warning displayed did not provide with sufficient information.

An empirical study on the effectiveness of phishing warnings revealed that 43% of participant (i.e. out of 47 respondents) did not comprehend the meaning of the warning that had been presented [10].

30 respondents were interviewed in relation to computer security warnings and it showed that the novice users often did not understand the technical terminology. These users always struggle to understand the meaning of the terminology because of the technicality and the difficulty of such terms [11]. In addition, the majority of respondents indicated that the novice users were unable to make informed decision about firewall warnings [12].

A big scale survey with 340 end-users on the usability of security software was conducted and it revealed that end-users find it difficult to understand the technical terminology. About 35% of the respondents were not able to understand the ActiveX jargon in Internet Explorer [13].

It can be concluded that end users are still facing different types of problem in relation to security warnings. It can be noted that the warnings issued are not fixed to one scenario but it covers different types of circumstances. Thus, the next section will explore the method or techniques that have been put in place to counter the problems.

B. *Methods to improve security warnings*

There is no one specific method to solve problems on security warnings. Researchers carried out various experimental studies on security warnings to explore the problems and possible solution. Table II presents a summary of studies on how to improve security warnings based on the early investigations that had been made [14].

TABLE II. SUMMARY OF STUDIES ON HOW TO IMPROVE SECURITY WARNINGS

Authors	Methods/Techniques
Nodder (2005)	Proposed a new design of warning based on users' behaviour
Raja et al. (2009)	Proposed a new firewall interface design that helped users to develop a correct mental model and increased users' understanding on firewall configuration.
Bravo-Lillo et al. (2011b)	Introduced the concept of mental model on how novice and advanced users assessed security warnings.
Keukelaere et al. (2009)	Introduced Adaptive security dialogues (ASD) by matching the complexity of warning dialogues and the risk associated
Edwards et al. (2007)	Introduced security automation concept where decision is made by the system
Bravo-Lillo et al. (2011)	Proposed design changes that are able to help end-users to make better decision in relation to warning interaction.
Kauer et al. (2012)	Proposed that the risk should be communicated clearly in order to deliver the message in secure manner,
Raja et al. (2011)	Proposed a design solution based on the physical security metaphor and Human In the Loop (HITL),
Brustoloni & Villamarín-Salomón (2007)	Introduced Polymorphic and audited dialogue to improve security warning decisions.
Villamarín-Salomón & Brustoloni (2010)	Introduced security reinforcing applications (SRAs) which rewarded end-user based on their behaviours.
Maurer et al. (2011)	Proposed new concept of warning design where it appeared together when user wanted to key in the data online.
Hardee et al. (2006)	Suggested that attributes or features should be utilised in security warnings
Stoll et al. (2008)	Introduced Sesame – visualisation system which showed to end-users the background process which were always hidden from them.

From this summary it can be seen that most of the methods improved security warnings by utilizing the features or attributes on warnings and by creating or designing new form of warnings. However, there is not much emphasis on new framework or architecture on security warning.

Table III provides information on problems that had been highlighted with the proposed solutions by various researchers [14]. There are six common problems related to security warnings (i.e. attention towards warnings, understanding of warnings, use of technical wordings, evaluation of risk from warnings, user's motivation towards heeding warnings and user's assessment of the implication of warnings).

TABLE III. COMMON PROBLEMS RELATED TO SECURITY WARNINGS AND THEIR SOLUTIONS

Common problems with security warnings	Proposed solutions
Attention towards warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Raja et al. (2011), Maurer et al. (2011) and Hardee et al. (2006).

Common problems with security warnings	Proposed solutions
Understanding of warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Edwards et al. (2007), Bravo Lillo et al. (2011), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Hardee et al. (2006) and stoll et al. (2008).
Use of technical wordings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Raja et al (2011) and Hardee et al (2006).
Evaluation of risks from warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Maurer et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's motivation towards heeding warnings	Bravo Lillo et al. (2011b), Bravo Lillo et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's assessment of the implication of warnings	Bravo Lillo et al. (2011b), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Villamarín-Salomón & Brustoloni (2010) and Stoll et al. 2008).

This classification is useful for the others to understand the initial problem and possible solution in relation to security warnings. It highlights useful literature review that had been gathered from the observation and initial studies.

C. *Approaches related to security warnings*

There are many different conceptualizations of warning process. Overviews of warning process can be discussed from the warning science literature angle to the specific method in relation to security warning studies. This section will explore computer related frameworks that suit the security warnings domain.

One of the most cited papers in relation to warning domain is Communication-Human Information Processing (CHIP) as in Fig 1 [15]. The framework highlights the steps in warning processes to identify the reasons for failures of one particular warning. By utilizing this framework, problems with the warnings process can be identified and later can be solved accordingly.

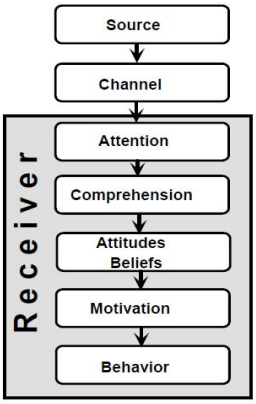

Figure 1. Communication-Human Information Processing Framework (C-HIP) [15]

Cranor was among the first researchers to use C-HIP model to develop the Human in the Loop (HITL) (Fig 2) security framework [16]. She used the CHIP as the basis to further enhance her own framework. HITL worked to identify security problems and helped to understand the end users' behaviors after performing security related functions.

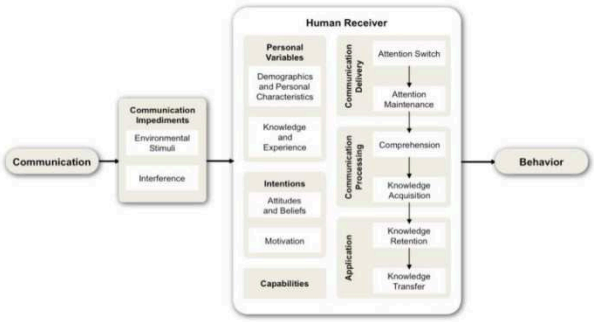

Figure 2. Human in the Loop Security Framework (HITL) [16]

Security related functions normally actuate through security-related communication (i.e. the first element in HITL) which can be derived from warning, notices, status indicator, training or policy.

Four main features are involved in HITL such as communication, communication impediments, human receiver and behavior. She grouped the communication impediments with environmental stimuli and interference and she classified human receiver with personal variables, intentions, capabilities, communication delivery, communication processing and application. Finally, the framework showed that the aim of security communication is to promote and to ensure safe behavior.

She also introduced a four step iterative process also known as Human Threat Identification and Mitigation Process as shown in Fig 3 [16]. It can be noted that HITL is part of the iterative process.

The task identification step involves system designer to identify whether the systems rely on human in order to perform security functions. Task automation step indicates whether security functions would be able to partially or fully automate. The failure identification step focuses on identifying the failure of security functions by utilizing the HITL framework and user studies. Finally, failure mitigation step prevents failures by identifying how users can be supported.

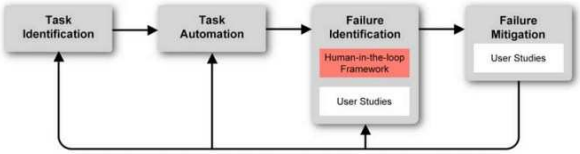

Figure 3. Human Threat Identification and Mitigation Process [16]

She applied her research study to this framework by using anti phishing tools (i.e. passive warning indicators in web browsers were not effective to prevent users from phishing sites). She revealed from her findings that there

is a need to find ways to correct users' mental model about phishing and proposed to focus on links to educational materials to improve anti-phishing warnings. She also recommended three high-level strategies to build a secure system for human beings to use as mentioned accordingly:

- To find ways to ensure human are out of the loop and build systems without involving human in security critical functions;
- To build systems that are intuitive and find method to make it easy to use;
- To teach human on how to perform the security critical task.

One notable advice that she mentioned was that individual or researchers cannot rely on one strategy to be successful. A combined approach is the best practice. One approach might not suit another situation. Therefore a combination will work better as it will support one another.

The Spectrum of automation approaches was introduced in 2007 [17]. It explained the strategies on how security automation for end-users can be implemented as shown in Fig 4. The fixed policy indicates that the security decision policies are in tool and application (e.g. Karberos server – security kernel implementation). The customised policy allows the policy to be added or customised (e.g. managed by the system administrator) and finally the dynamic policy works in a flexible manner with dynamic policy adaptation (e.g. Bayesian spam filters).

In relation to security warnings, it can be suited to the spectrum the security warnings identified. With this approach, the decision making process will be much simpler as the decision is made automatically by the system. However, full consideration must be put in place as there are many challenges that limit the automation. For example, the social and environmental contexts of security must be considered. In addition, the consequences of security automation on end users would be a critical agenda to be highlighted.

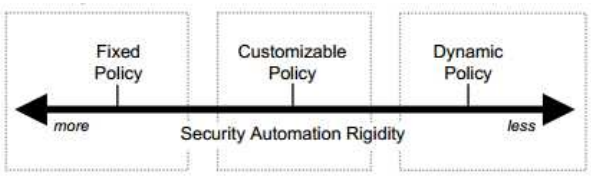

Figure 4. The Spectrum of Automation Approaches [17]

Another approach is system visualization. It is used as a tool to provide more information to end users by highlighting how each process works in the computer system. However, not very much focus has been given on this area. Sesame was introduced as an interactive visualisation concept in order to help non-expert users make informed security decisions [18].

Sesame works by utilizing the desktop metaphor in order to show the background process when users wants to make security decision. Every steps involved will be shown to the users so that they will be able to comprehend 'behind the scene' scenarios (i.e. the technical process involves). The result of system visualisation is convincing as system activity, configuration and action can be viewed easily and better apprehended [19].

D. *Classification of security warnings approaches*

After understanding the problems and the proposed solution of security warnings, this section highlights how each approach can be grouped or classified based on the techniques used. After gathering all information and evidences, four classifications are introduced (Fig. 5) [14]:

- Redesign the warnings by utilising the features and available information in the warnings
- Redesign the warnings by behaviour modification.
- Redesign the warnings by changing the presentation or layout
- Redesign the warnings by the adaptation of warnings

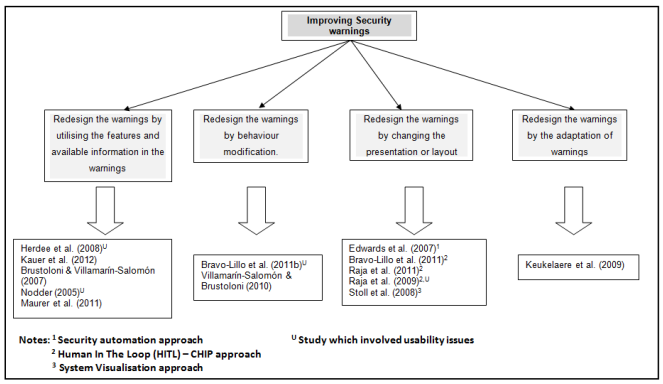

Figure 5. Classification Approaches to Improve Security Warnings [14]

It can be noted that most of these findings were focusing on the redesign warnings. Warnings should be designed in a way that it will promote secure manner actions. In addition, users encounter the security warnings on daily basis which indicates the importance of delivering correct information and advise so that they are aware of possible menaces and possible action to take.

Based on Fig 5, most researchers had focused on the first three classifications. However, "Redesign warnings by the adaptation of warnings" seem to be an unpopular one. Adaptive Security Dialog (ASD) fulfils the last classification to improve security warnings dialogs by producing a new architecture in order to promote a new type of interaction [20]. As the underlying cause of the security warnings problem had been addressed, it indicates there is a necessity to design security warnings in a way that can suit researchers' Goal and objectives.

III. DISCUSSION

Earlier, problems in relation to security warnings had been highlighted. Even though the problems ware not thoroughly discussed but it provides some overview of problems faced by the end users. Table II and Table III

show information and evidences to indicate what had been done to improve security warnings. Apart from that, researchers had demonstrated various techniques or methods to provide possible panacea in warning studies. As a result, the classification approach to improve security warnings is presented.

To our knowledge, there has been no similar compilation of information or overview in relation to security warning studies. Therefore, we took the initiative to provide this platform so that we can share this useful information.

All of this information is useful for individual or researchers in security warnings domain. They can use this as a guide and as part of their literature review process. It is a challenging process to gather all these evidence and we hope that it will give positive benefits to others undertaking research in this area of study and to the general public.

IV. Conclusion

In conclusion, problems in relation to security warnings studies had been highlighted. The findings from the earlier survey studies have motivated our work in the area [14]. In addition, the possible solutions are presented based on the classification of the mentioned problems. Suitable approaches had been described accordingly based on suitability of the problems. The classification of approaches can be considered as a new element in security warning studies which provides the benefits to the research community and to the general public.

V. References

[1] Wogalter, M.S. "Purposes and Scope of Warnings, In *Handbook of Warnings*. (Human Factors /Ergonomics)" (Assoc LE, Ed), 2006, pp. 3-9, ISBN 0805847243.

[2] Tuchscheerer, S., Dittmann, J., Hoppe, T. and Krems, J. F. "Theoretical analysis of security warnings in vehicles and design challenges for the evaluation of security warnings in virtual environments', *Proceedings of the First International Workshop on Digital Engineering*", 2010, Magdeburg, Germany. ACM, pp. 33-37.

[3] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. & Cranor, L. F. "Crying wolf: an empirical study of SSL warning effectiveness", *Proceedings of the 18th conference on USENIX security symposium*. 2010, Montreal, Canada USENIX Association, pp. 399-416.

[4] Weir, C. S., Douglas, G., Carruthers, M. and Jack, M. "User perceptions of security, convenience and usability for ebanking authentication tokens", *Computers & Security*, 2009, vol.28, 1-2, pp. 47-62.

[5] Lampson, B. "Privacy and security: Usable security: how to get it", *Communication of ACM*, 2009, vol.52, 11, pp. 25-27.

[6] Nodder, C. "Users and Trust: A Microsoft Case Study". In Cranor, L.F. and Gar-finkel, S. (eds) *Security and usability. Designing Secure Systems That People Can Use*. O'Reilly, 2005, pp. 589-605, ISBN 0596008279.

[7] Microsoft. "Windows User Experience Interaction Guidelines"[Online]. 2010. Available at: http://msdn.microsoft.com/en-us/windows/aa511258.aspx

[8] Wu, M., Miller, R. C. & Garfinkel, S. L. "Do security toolbars actually prevent phishing attacks?" *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006, Montreal, Quebec, Canada ACM, pp. 601-610.

[9] Seifert, C., Welch, I. & Komisarczuk, P. "Effectiveness of security by admonition: a case study security warnings in a web browser setting", *secure Magazine*, 2006, pp. 1-9

[10] Egelman, S., Cranor, L. F. & Hong, J. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings", *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. 2008, Florence, Italy ACM, pp. 1065-1074.

[11] Bravo-Lillo, C., Cranor, L. F., Downs, J. S. & Komanduri, S. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach", *Security & Privacy*, 2011, IEEE, vol.9, 2, pp. 18-26.

[12] Raja, F., Hawkey, K., Hsu, S., Wang, K. L. C. & Beznosov, K. "A brick Wall, a Locked Door, and a Bandit: A physical Security Metaphor For Firewall Warnings", *Proceedings of the Seventh Symposium on Usable Privacy and Security*. 2011, Pittsburgh, USA, ACM, pp. 1-20.

[13] Furnell, S. M., Jusoh, A., Katsabas, D. & Dowland, P. S. "Considering the Usability of End-User Security Software", *Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006). 2006,* Karlstad, Sweden. Springer Boston, pp. 307-316.

[14] Zaaba, Z. F. "Enhancing Usability using Automated Security Interface Adaptation (ASIA)" PhD Thesis, 2014, University of Plymouth.

[15] Wogalter, M. S., Dejoy, D. M. & Laughrey, K. R. "Organizing Theoretical Framework: A Consolidated Communication-Human Information Processing (C-HIP) Model". In Wogalter, M.S., Dejoy, D.M. and Laughrey, K.R. (eds.) *Warning and Risk Communication*. 1999 Taylor & Francis, pp. 13-21. ISBN 0748402667.

[16] Cranor, L. F. "A framework for Reasoning About the Human in the Loop", *USENIX : Usability, Psychology and Security (UPSEC),* 2008, San Francisco, USA, pp. 1-15.

[17] Edwards, W. K., Poole, E. S. & Stoll, J. "Security Automation Considered Harmful", *Proceedings of the 2007 Workshop on New Security Paradigms*. 2007, North Conway, USA, ACM, pp. 33-42.

[18] Stoll, J., Tashman, C. S., Edwards, W. K. & Spafford, K. "Sesame: informing user security decisions with system visualization", *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. 2008, Florence, Italy, ACM, pp. 1045-1054.

[19] De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Rien, J., Rode, J. A. & Filbo, R. S. "In the eye of the beholder: A visualization-based approach to information system security", *International Journal of Human-Computer Studies*, 2005, vol.63, 1-2, pp. 5-24.

[20] Keukelaere D. F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L. & Zurko, M. "Adaptive Security Dialogs for Improved Security Behavior of *Users", Human-Computer Interaction – INTERACT 2009'.* 2009, Springer Berlin / Heidelberg, pp. 510-523.