PAINLEsS – Personalized Multimodal Persuasive Ambient and Peripheral Interaction for Information Security

Marc Busch
CURE – Center for Usability
Research & Engineering
1110 Vienna, Austria
busch@cure.at

Peter Wolkerstorfer
CURE – Center for Usability
Research & Engineering
1110 Vienna, Austria
wolkerstorfer@cure.at

Christina Hochleitner
CURE – Center for Usability
Research & Engineering
1110 Vienna, Austria
hochleitner@cure.at

Manfred Tscheligi
University of Salzburg
5020 Salzburg, Austria
manfred.tscheligi@sbg.ac.at
&
AIT – Austrian Institute of
Technology GmbH
1220 Vienna, Austria
manfred.tscheligi@ait.ac.at

Abstract

Violations against information security policies in organizations caused by employees are frequent and expensive. Classical countermeasures, such as security training and education, as well as awareness campaigns only have a limited and short-term effect on the employees' information security policy attitudes and compliance. Additionally, they are time-consuming, expensive and don't comply with employees hedonic needs. To promote a positive and long-lasting increase of information security policy awareness and compliance we propose an innovative framework (PAINLEsS), which can be implemented in organizations and consists of sensors that detect violations against security policies and multimodal peripheral feedback, which educates users and raises awareness about/for secure behavior via personalized persuasive ambient strategies.

Author Keywords

Information Security Policies; Security Training/Education/Awareness; Multimodal Ambient/Peripheral Interaction; Persuasion

ACM Classification Keywords

H.1.2 User/Machine Systems: Human factor

Introduction

According to a PWC survey[1] in the United Kingdom, 93% large and 87% small organizations had a security breach in the last year. These numbers have increased from year to year. Not only external attackers cause these security breaches: 36% of the worst security breaches in a year were caused by human error of the organization's employees. Neither technological approaches, nor human approaches (security education, training and awareness programs [SETA]) alone have been really successful: Employees know how to avoid technological approaches and SETA programs are obtrusive, time-consuming, and expensive, not directly in the context of information security breaches and have only short-term effects or must be administered repeatedly to have long-term effects. Additionally, they often don't contribute to a positive experience with information security compliance. Furthermore, employees are not aware of SETA programs or do not feel the wish to participate in such [7]. SETA programs are designed as a "one fits all" model, neglecting individual differences between employees.

The Way Forward: PAINLEsS

Therefore, we propose an innovative framework that incorporates all these requirements and makes use of personalized persuasive peripheral and ambient feedback strategies. The goal is to change the employees' information security behavior through subtle peripheral cues. We believe that such cues provided through different modalities have the potential to persuade users towards this goal.

PAINLEsS (Personalized Multimodal Persuasive Ambient INtelligEnce for Information Security at the Workplace) will make use of different hard- and software sensors to provide contextual information to a security policy monitoring and alerting system. The sensor data is processed along with the security policies to detect breaches of those. Security breaches within the PAINLEsS framework refer to breaches (of the security policies) from employees (not from unauthorized outsiders). An example is the storage of unencrypted organizational data on the employees' mobile devices. From a breach of the security policies follows a personalized, multimodal, ambient and peripheral feedback about the user's security behavior. Sensor data includes lighting conditions, pressure sensors on the seating areas of chairs, but also cameras (to capture emotional reactions to personalize the systems' effectiveness).

The tailored multimodal and subliminal messages consist of visual cues, tactile stimulation, sound and scent - an underused modality in HCI [6]. Through the sensors' contextual data PAINLEsS will learn about (combinations) of subliminal messages that have a positive impact on security behavior. We hope to overcome the shortfalls of more cognitive and central approaches (e.g. technological and SETA approaches) with PAINLEsS and provide a holistic and positive information security experience to employees.

The Concepts of PAINLEsS

Personalized Persuasive Technology is technology that aims at changing user attitudes and behavior towards in a certain domain (e.g. corporate information security) [2] by the implementation of a variety of persuasive strategies, e.g. by self-monitoring (help the

[1] http://www.pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pdf

user to keep track of performance, status or goal achievements) and is tailored to the users' individual personality [1,5]. Persuasive Technology has been rarely used in the area of information security [10]. Environmental Persuasion is persuasion that aims at a more unconscious persuasion that comes from the environment. For example: [8] suggests to implement a translucent digital interface as stairs in a subway to persuade people to take the stairs instead of an escalator. Environmental Persuasion is strongly related to Peripheral and Ambient Interactions. These are interactions with technology, which occur outside the central focus of the attention and fluently blend into everyday life.

The PAINLEsS workplace

Our general approach is to overcome the utilitarian and more productivity-oriented notion of information security and increase compliance through hedonism [4]: users want to avoid unpleasant situations. Hence we expect them to behave in a way to change unpleasant situations back to pleasant ones and to be motivated through positive experiences.

Inspired by translucent stairs in a subway to promote stair climbing [8], employees have translucent writing desks, which can gradually change color from pleasant to unpleasant colors according to their security policy compliance. Not only the desks will change color, also parts of the employee's clothing will indicate security breaches [9]. Employees will be interviewed and observed to find out which color has positive/negative connotations to them to really personalize the experience. [3] have shown that lamps that gradually change color can be more effective in persuasion than factual feedback. The persuading factor, as we hypothesize, is the color: users will try to get back to a pleasant color and get rid of the more unpleasant color. PAINLEsS adapts methods for vibro-tactile [11] feedback originally used for seated posture guidance and develops an office chair, which informs users in about security breaches: Through vibration, thermal changes and movement. Over time, the PAINLEsS framework is able to learn about the user's behavior and can apply a range of personalized feedback combinations. For scent as feedback, PAINLEsS will learn through the analysis of the combination security breach and sensor data, which scents evoke positive/negative behavior. PAINLEsS will create an ambient soundscape which can also range from pleasant to unpleasant and changes according to security breaches. The soundscape will be chosen from a set of possible sounds, based on user preferences.

We see peripheral and ambient interaction and feedback at the workplace as a possibility to enhance the employees' experience in a positive way and to engage users in a hedonic way to comply with security policies. Our position is, that the personalized combination of different peripheral and ambient feedback modalities has a strong persuasive effect on the employees: Tailored light, tactile stimulation, scent, and sound are able to evoke strong emotions in the employees. We believe that the integration of emotions (through the described subliminal feedback) to promote security policy compliant behavior (detected by the security monitoring system) will be more effective than more cognitive and direct approaches (such as security trainings and awareness campaigns). The ongoing unobtrusive peripheral feedback is expected to have more influence than factual (e.g., security-warning pop-up windows on a screen) security feedback.

Unobtrusiveness and the lack of paternalisation are the user-experience factors, which make us believe, that our solution will have more impact than the classical SETA approach. We also believe that the presence of the security feedback (which is subtle, but lasting as long as user behavior changes) tends to increase the user's curiosity about his/her own behavior. We expect that in order to gain positive and hedonic experiences, users will be motivated to change the modalities that are provided by their workspace (e.g. light, scent) into comfortable states and learn to comply with security policies. However, these modalities also depend on the context and preferences may change over time.

Discussion and Future Research

A limitation and crucial point in the PAINLEsS framework are certainly the legal and ethical implications: The nature of peripheral and ambient interaction at the workplace exposes the employees' security behavior to other employees and also to superiors. This is a fundamental intervention into personal privacy and has to be considered in the design of the framework. The framework should not blame or expose employees in front of their colleagues. In the future, we will conduct user research to examine if every component of the PAINLeSs framework is effective at raising security awareness and behavior and how it should be personalized. Then we will implement a first prototype in a company and evaluate it in a field study.

Acknowledgements

This work was partially funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement 318508 (MUSES – Multiplatform Usable Endpoint Security).

References

1. Busch, M., Schrammel, J., and Tscheligi, M. Personalized Persuasive Technology – Development and Validation of Scales for Measuring Persuadability. In *Persuasive Technology*. Springer Berlin Heidelberg, 2013, 33–38.
2. Fogg, B.J. *Persuasive Technology - Using Computers to Change What We Think and Do*. Morgan Kaufmann, 2002.
3. Ham, J., Midden, C., Maan, S., and Merkus, B. Persuasive lighting: The influence of feedback through lighting on energy conservation behavior. (2009).
4. Heijden, H. Van der. User acceptance of hedonic information systems. *MIS quarterly 28*, 4 (2004), 695–704.
5. Kaptein, M.C. Personalized persuasion in Ambient Intelligence. *Journal of Ambient Intelligence and Smart Environments*, (2012).
6. Kaye, J. "Jofish." Making Scents. *interactions 11*, 1 (2004), 48–61.
7. Lebek, B., Uffen, J., Breitner, M.H., Neumann, M., and Hohler, B. Employees' Information Security Awareness and Behavior: A Literature Review. *2013 46th Hawaii International Conference on System Sciences*, IEEE (2013), 2978–2987.
8. Mathew, A.P. Using the environment as an interactive interface to motivate positive behavior change in a subway station. *CHI '05 extended abstracts on Human factors in computing systems - CHI '05*, (2005), 1637.
9. Wakita, A. and Shibutani, M. Mosaic textile: wearable ambient display with non-emissive color-changing modules. *CHI'06* , (2006).
10. Yeo, A., Rahim, M., and Ren, Y. Use of Persuasive technology to change end user's IT security aware behavior: a pilot study. *International Journal of Human and Social Sciences*, (2009), 673–679.
11. Zheng, Y. and Morrell, J. Comparison of Visual and Vibrotactile Feedback Methods for Seated Posture Guidance. (2012).