Behavior Change Support Systems for Privacy and Security

Roeland H.P. Kegel and Roel J. Wieringa

University of Twente, Enschede, The Netherlands

Abstract. This article proposes to use Behavior Change Support Systems (BCSSs) to improve the security of IT applications and the privacy of its users. We discuss challenges specific to BCSSs applied to information security, list research questions to be answered in order to meet these challenges, and propose an architecture for the Personal Information Security Assistant (PISA), a software framework designed to improve the privacy-related behaviors of end-users.

1 Introduction

Research into BCSSs has mostly been applied in the context of healthcare: persuading users to adopt a healthier lifestyle, or to comply with medical advice. However, another potentially fruitful area of application is information security: digital systems and services are becoming more complex and connected, and thereby become more vulnerable. After technical risk mitigations have been implemented, the human element often turns out to be the weakest link in the information security chain. Risk perceptions in information security are strongly influenced by incidents [1, 2]. A BCSS can help improve the alignment between risk perceptions and reality in the absence of recent incidents. However, BCSSs in information security differ from healthcare in that positive feedback is the absence of consequences (no security breaches), and in security there may be a long delay between action and consequence (the security breach can happen months after the behavior that caused it). This means that any BCSS for information security will need to address several domain-specific challenges. There are few publications on the application of BCSS to security. One of these is by Johnston, listing 10 general requirements for security interfaces[3]. In the Personal Information Security Assistant (PISA) project[1], we aim to reduce security risks and enhance the privacy of users by persuading them to change their attitudes and behaviors in this area. We do this by offering a personalised security operations center for the individual: the PISA.

2 Challenges in the Application of BCSS to Security and Privacy

Based on previous discussions with experts in Risk Assessment, as well as established end-user security literature such as [3], we define two challenges in the

[1] http://scs.ewi.utwente.nl/projects/pisa/

field of end-user security. We then associate these challenges with corresponding goals that we think have the potential to meet them.

Challenge: Motivation and change type The Elaboration Likelihood Model (ELM)[6] defines the constructs *user ability* and *motivation*, which influence what type of communication will be effective. We assume that both ability and motivation to improve IT security and privacy are low among the general public, and so a BCSS for security and privacy needs to employ persuasive techniques that require little intervention or thought from the user. Such a communication strategy relies on the ELM's *peripheral route*, where users use heuristics and peripheral cues to make their decisions. However, directly conflicting with this strategy is the type of change that PISA needs to achieve: sustained behavioral and attitudinal change is needed to raise security awareness[1]. This type of change is best realised through education and intervention. Such a strategy corresponds to the ELM's *central route*, relying on careful thought and consideration from the user. This conflict in route choice leads us to define the following goal:

Goal: Personalisation A BCSS for security and privacy needs to personalise the interaction with its users, allowing for the maximum of education and interaction that users are comfortable with, based on their motivation and ability. Personalisation also allows dialogue to evolve over time as user's attitudes and abilities change. A BCSS can do this by observing the user's actions and behavior when interacting with digital systems and services. Based on this information, the BCSS should be able to estimate the user's risk appetite and security preferences.

Challenge: Dynamic threats Security and privacy can be compromised by a vast range of threats. Most of these threats require sophisticated technology and expertise to address. In addition, these threats are dynamic and change over time, which means countermeasures will need constant maintenance. A be-all-end-all system for security, then, is not feasible. This leads to the second goal for a security- and privacy-enhancing BCSS:

Goal: An extensible software framework Since privacy cannot be protected by a single system, a different approach is needed. Using a software framework that can integrate multiple extensions to protect against different threats can be an answer to this problem. Using different extensions for different threat categories, education and motivation regarding privacy can still be achieved using a single system. This way, a BCSS can offer a robust platform for sharing system information, user activity and a single channel for communicating with a user. This allows for a better user experience, minimizing redundant communciation between protective systems and the user. Additionally, such a framework can form the basis for an ecosystem of protective measures developed by different parties, distributing the development and maintenance cost of a comprehensive security solution.

3 Research Questions

The goals defined in the previous section lead us to the following research questions specific to a BCSS as applied to information security and privacy:

Q1: How can user ability and motivation regarding information security be measured by observing human computer interactions? The answer to this question is needed to address the personalisation goal: to structure the message in a clear and persuasive manner, both constructs need to be taken into account.
Q2: What user-characterising factors can and should influence how a BCSS takes action and informs the user? The answer to this question is also needed for the personalisation goal: beyond motivation and ability, many factors can influence how a person responds to information presented by the BCSS. Identifying and incorporating them will enhance the system's persuasive ability.
Q3: How can enterprise risk assessment methodologies be adapted for and applied by end-users to enhance the security of the IT systems they use, and/or their own privacy? The answer to this question well help us structure educational content for effecting behavioral change in security and privacy: a wealth of risk assessment methodologies exist for an enterprise context. If a way can be found to adapt this to an end-user context, the message itself can be improved, heightening effectiveness as well as credibility of the BCSS.
Q4: How can a user's personal and system security status be visualised? Implementing the answer to this question will improve the persuasive power of the BCSS: without an effective way to communicate a user's status, it becomes hard to motivate users to change their behavior.
Q5: What techniques can be used to maintain the privacy of a user's data while allowing cross-extension communication? This question needs to be answered in order to prevent a security and privacy BCSS from becoming a risk of its own: consolidating a wealth of intelligence on a person risks making the BCSS a single point of failure in security.

4 PISA Architecture

The goal of the PISA is to enhance user privacy by persuading the user to change their behavior in accordance with their privacy risk appetite. Previously, we have used the Persuasive Systems Design (PSD) model by Oinas-Kukkonen[5] to identify requirements and persuasive elements of the second PISA prototype [4]. After developing two prototypes, we have converged on the architecture shown in Figure 1.

The PISA Client: A program running on a user's device. Interacts with the user and uses information gathered from sensors in PISA extensions to keep a user profile up to date. Based on this user profile and a database of rules, PISA protects the user when an event takes place. It does this through advice to the user and by using actuators in PISA extensions.

PISA Extensions: Plugins that can integrate with PISA, protecting the user based on a set of event-response rules associated with the PISA Extension. Sensors are programs that can monitor aspects of the user's system (such as browsing activity or typing speed) while Actuators are programs that can take specific actions within a user's system (such as starting a virus scanner). The Logic component is a program that communicates between different parts of the extension and the PISA client.
The PISA Update Server: A centralized database of plugins and event-response rules that the PISA Client can use to update itself.

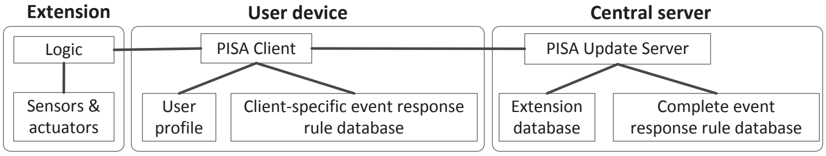

Fig. 1. The architecture of the PISA

As a proof of concept, our second prototype used a browser plugin as a PISA extension to detect when a user was entering his password on a non-HTTPS protected site. It then informed the user and prevented him from entering his password on what could potentially be a phishing site.

5 Planned Work

This architecture will be used as a guideline for implementing a series of prototypes that we will test in laboratory conditions (using students and researchers as subjects), using feedback from each iteration to improve the next. The immediate research question that these prototypes will aim to answer is how to assess a user's skill and motivation based on observation (Q1 and Q2). When personalisation is possible, advice and educative content and human-computer dialogue will be structured using enterprise risk assessment methods (Q3). Once sufficient extensions exist, a test involving a tiered reporting structure, aggregating sensor data into categories, will be used to visualise the observed risk appetite of the user (Q4). Existing literature on privacy preserving techniques will be consulted throughout the development of the extension API (Q5). Finally, a test of the efficacy and persuasive elements of the prototype will be carried out in a real world context with our project partners, which include an internet service provider and a telecom service provider.

Acknowledgments The PISA project is sponsored by NWO and KPN under contract 628.001.001.

References

1. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empiricial study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523 – A7 (2010)
2. Gonzalez, J.J., Sawicka, A.: A framework for human factors in information security. In: WSEAS International Conference on Information Security, Rio de Janeiro. pp. 448–187 (2002)
3. Johnston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Computers & Security 22(8), 675 – 684 (2003)
4. Kegel, R.H.P., Wieringa, R.J.: Persuasive technologies: a systematic literature review and application to pisa. Technical Report TR-CTIT-14-07, Centre for Telematics and Information Technology, University of Twente, Enschede (May 2014)
5. Oinas-Kukkonen, H., Harjumaa, M.: Persuasive systems design: Key issues, process model, and system features. Communications of the Association for Information Systems 24(1), 485–500 (2009)
6. Petty, R., Cacioppo, J.: The Elaboration Likelihood Model of Persuasion, Advances in Experimental Social Psychology, vol. 19, pp. 123–205. Elsevier (1986)