Performance Evaluation 98 (2016) 36–51

Contents lists available at ScienceDirect

Performance Evaluation

journal homepage: www.elsevier.com/locate/peva

Modeling and analysis of influence power for information security decisions

Iryna Yevseyeva [a,b,*], Charles Morisset [a], Aad van Moorsel [a]

[a] *Centre for Cybercrime and Computer Security, School of Computing Science, Newcastle University, Newcastle upon Tyne NE1 7RU, UK*
[b] *Faculty of Technology, De Montfort University, Gateway House 5.33, The Gateway, LE1 9BH Leicester, UK*

ARTICLE INFO

Article history:
Available online 19 January 2016

Keywords:
Information security
Security–productivity trade-offs
Multicriteria decision analysis
Influencing behavior
Nudging
Influence power

ABSTRACT

Users of computing systems and devices frequently make decisions related to information security, e. g., when choosing a password, deciding whether to log into an unfamiliar wireless network. Employers or other stakeholders may have a preference for certain outcomes, without being able to or having a desire to enforce a particular decision. In such situations, systems may build in design nudges to influence the decision making, e. g., by highlighting the employer's preferred solution. In this paper we model influencing information security to identify which approaches to influencing are most effective and how they can be optimized. To do so, we extend traditional multi-criteria decision analysis models with *modifiable criteria*, to represent the available approaches an influencer has for influencing the choice of the decision maker. The notion of *influence power* is introduced to characterize the extent to which an influencer can influence decision makers. We illustrate our approach using data from a controlled experiment on techniques to influence which public wireless network users select. This allows us to calculate influence power and identify which design nudges exercise the most influence over user decisions.

1. Introduction

People continuously make information security decisions: should I use a particular public wireless, should I allow someone's USB to be put in my laptop, how do I choose and memorize passwords? The decisions are often complex, with several objectives to be considered simultaneously, and the optimal decision may very much depend on the specific situation: while using a stranger's USB stick is not advisable, the importance of the job to be completed and/or knowledge about the owner of the USB stick may make it reasonable to use it, despite the associated information security risks.

A simple compliance policy (such as, not to allow USB sticks at all) would be suboptimal. Instead, one would want to allow the owner of the laptop to decide the best course of action. This also emerges in recently popular bring your own device (BYOD) strategy [1] which many companies follow. BYOD strategy assumes device owners use their own devices for work-related activities. The fact that the user owns the device puts certain restrictions on what the employer can do to implement its preferred security solution. In any case, there are many situations in which the end user is involved in information security decisions that impact other stakeholders.

Although various stakeholders are not in a position to control the outcome of the information security decision, it may be advisable that some stakeholders (e.g., service providers, device vendors, employers) impacted by the end-user decisions are

[*] Corresponding author at: Faculty of Technology, De Montfort University, Gateway House 5.33, The Gateway, LE1 9BH Leicester, UK.
E-mail addresses: Iryna.yevseyeva@dmu.ac.uk (I. Yevseyeva), Charles.Morisset@newcastle.ac.uk (C. Morisset), Aad.vanMoorsel@newcastle.ac.uk (A. van Moorsel).

http://dx.doi.org/10.1016/j.peva.2016.01.003
0166-5316/© 2016 Elsevier B.V. All rights reserved.

able to *influence* the decision making, without restricting the freedom of choice of the end-user. Influencing techniques (such as nudging [2]) have been widely used in marketing, healthcare and social policies, see e.g. [3–5], but less so in information security. To establish a sound base to design, evaluate and optimize influencing techniques in information security, a formal and coherent framework to analyze and evaluate influencing is needed.

In our earlier work [6], we identified an agent-based model that allows one to reason conceptually about influencing information security. The general notion of optimal influencing policy was introduced, taking into account uncertainty of the environment and the fact that agents have partial and differing abilities to observe that environment. The paper shows that end-user decisions under influencing may outperform the decisions made by either the end-user or influencer alone (in terms of [6], it shows that 'soft enforcement' can be better than weak or strong enforcement).

In this paper we seek a more operational model that allows us to identify which approaches to influencing are most effective for real-life scenarios and how these approaches can be optimized. To this end, we apply and extend well-known models from multi-criteria decision analysis, a well-understood and frequently used approach to modeling human decision making, see e.g. [7]. In our model, both decision-maker and influencer make decisions governed by multi-attribute value theory [8]. To represent influencing *modifiable criteria* are introduced here. Modifiable criteria reflect the impact an influencer has on the decision maker but do not change the available alternatives to chose from. For instance, if the influencer uses colors when presenting alternatives, the coloring does not change which options are available but does influence the value the decision makers associates with its decision criteria.

The notion of *influence power* is also introduced. Influence power expresses the extend to which a user is susceptible to being influenced, in terms of individual criteria. Vice versa, by adding a cost function to modifying criteria, influence power also allows one to express the effort needed by the influencer to successfully change the user's decision. That is, influence power allows one to evaluate and compare the effort needed in influencing approaches and therefore provides a tool to optimize the design and application of an influencing approach.

To illustrate the use of the concepts introduced in this paper we parameterize a model using data from a controlled experiment in WiFi network selection [9]. The experiment provides data about a number of design nudges which aimed at influencing which WiFi network would be selected. These design nudges include coloring of available networks, changing the order they are presented, etc. It is shown how the influence power of a particular criterion can be computed and how much influence power is needed to change the choices of participants with different preferences. We are able to determine whether the influencer can change the choice of decision makers by changing only one criterion at a time or a (sub)set of modifiable criteria. Such insights can guide the designer of nudges and improve the effectiveness of techniques for influencing choice.

The work presented in this paper improves on most elements of our earlier work in [10], which was the starting point for this special issue paper. The formalization is extended with the notion of influence power and with that of modifiable criteria. The analysis using experimental data from a study of nudging in public Wi-Fi network selection has been extended considerably, in particular through results in Section 5. We also extended the related work discussion, especially targeting the community of probabilistic system modelers, and we provided a much deeper discussion of remaining challenges and opportunities.

The paper is organized as follows. Before introducing our modeling approach, Section 2 discusses key elements of the state of the art in influencing techniques, drawing from literature in various disciplines. It also discusses related modeling approaches (particularly Markov decision models and reinforcement learning). Section 3 introduces our structured approach to modeling influence, including the concepts of influence power and modifiable criteria. Section 5 provides the data analysis for the WiFi network selection experiment, preceded by an explanation of the case study specifics in Section 4. We discuss gained insights in Section 6, referring to a number of interesting issues for further research and refinement, including intuitive decision making strategies, influencing through a 'decoy' alternative, and influencing a larger population of users. Section 6 provides the final conclusions.

2. Background and related work

Before presenting our approach to modeling influence, Section 2.1 provides a background discussion of influencing techniques in general and Section 2.2 positions our approach of using multi-criteria decision making when compared to Markov decision modeling and reinforcement learning.

2.1. Influencing decision making

Influencing decision making has attracted attention of researchers from many fields, including psychology, behavioral economics, marketing, health and, more recently, privacy and security. The research in these varying domains all discuss, from their own disciplinary perspective, the factors that influence choices and the design of interventions to try to influence decisions. Examples of such interventions are wide-spread, for instance interventions that aim to change smoking or eating habits [4]. In marketing, influencing is part and parcel of anything it aims to achieve, whether it is to improve product sales or protect the customer [11].

In recent times, policy makers have become increasingly interested in a specific instance of influencing, namely *nudging*, which was made popular by the work of Thaler and Sunstein [2]. Nudging refers to the design of a *choice architecture*, the