Assessing the Value of Formal Control Mechanisms on Strong Password Selection

Jeff Crawford, School of Computing & Informatics, Lipscomb University, Nashville, TN, USA

ABSTRACT

Applications often use behavior control mechanisms in order to ensure that individuals create sufficiently strong passwords. Behavior controls, which force individuals to utilize specific password characteristics, are assumed to be the best mechanism to encourage strong password creation. However, an over reliance on them could lead to counterproductive security behaviors. This study examines the efficacy of formal controls in the password creation process to determine if their use does indeed result in meaningfully stronger passwords than informal control techniques. Findings demonstrate that controls used during the password creation process do indeed shape password strength, but that behavior controls do not produce significantly stronger passwords than informal controls. Using an Agency Theory perspective, control techniques are considered in their ability to align principal-agent goal and risk perceptions. Findings illustrate the importance of using both informal and formal controls as a means of creating strong and effective passwords.

Keywords: Agency Theory, Behavior Controls, Control Theory, Information Security, Strong Passwords

INTRODUCTION

Passwords are a part of everyday life for most individuals. Whether using software at work or home, passwords are frequently used to secure digital resources with the critical assumption that strong passwords will decrease the likelihood of those resources being compromised. Despite a common outcry that passwords are an ineffective means of protecting identity (Herley, van Oorschot, & Patrick, 2009), there is a strong focus within the current application design paradigm to build systems that rely on users creating and maintaining passwords. The primary means of encouraging strong passwords is to utilize formal controls during the password creation process – e.g., requiring the use of specific password characteristics (e.g., # of characters, inclusion of specific types of characters, preventing the use of previous passwords, etc.) before allowing a password to be saved. Implementing formal controls during the password creation process seems appropriate given past evidence about the types of passwords that individuals often utilize. A recent examination of 32 million passwords
that were stolen from RockYou, an organization that designs social media games, found that user passwords frequently violated the site’s password recommendations. The most common password being used on the site at the time of the password breach in December, 2009, was ‘123456’ (The Imperva Application Defense Center, 2010). This finding gives credence to the use of formal controls as a means of encouraging strong password selection. Indeed, formal controls have become the de facto standard for ensuring that end users comply with strong password requirements.

Of utmost concern is the suggestion that while formal controls force an individual to utilize specific password characteristics, they might not encourage effective security minded behavior. This is especially concerning since formal password enforcement mechanisms place a considerable burden on end users, often producing less than optimal security behaviors (Herley, 2009). For example, individuals on average own 25 different passwords (Florencio & Herley, 2007), most of which are required to be strong. While the within application password creation process can force the individual to create a password with specific characteristics, individuals are incented to ‘game the system’ across applications as a means of reducing overall complexity (e.g., utilizing a common password across multiple sites). By forcing password policy compliance without addressing an individual’s underlying motivation, there is a potential for deviant behavior that can nullify or harm the positive effects of requiring strong passwords. In other words, failing to encourage the ‘why’ in strong password creation can encourage individuals to take shortcuts that detract from the rationale behind strong password use.

As such, the use of formal controls must be evaluated based on their actual effectiveness in the password creation process. If formal controls do not offer a clear advantage over informal controls in creating a strong password, then any disadvantages associated with utilizing behavior controls could make its exclusive use prohibitive. The present study seeks to address the degree to which different control techniques are effective during the password creation process. Specifically, this research examines whether behavior controls frequently used during the password creation process actually result in passwords that are strong above less utilized informal control techniques (e.g., self and clan). If there is not a meaningful difference in password strength, then a de facto reliance on behavior controls should be reconsidered.

The paper proceeds as follows. First, the use of different control types during the password creation process will be discussed, with a specific focus on the most common types of implemented control techniques. To properly frame this discussion, control theory will be discussed as a means of understanding the expected impact of various control mechanisms on password creation behavior. Research hypotheses are then tested and results discussed. The paper concludes by discussing implications, limitations, and future directions.

A CONTROL PERSPECTIVE ON THE CREATION OF STRONG PASSWORDS

Application designers have long recognized the importance of encouraging end users to create strong passwords. To this end, two general control techniques are typically applied with varying effectiveness. First and simplest is drawing on an individual’s desire to effectively secure his or her own digital resources. To accomplish this, application designers often attempt to educate end users by informing them about the consequences of poor password choice while also providing recommendations on how to create a ‘strong’ password. For example, Microsoft provides an on-line site for end users that utilizes a number of suggestions to encourage the use of strong passwords (Microsoft, 2011). Second, password creation mechanisms are often designed to require specific characteristics (e.g., minimum number of characters) before allowing the individual to save the password.
Related Content

Meta-Modeling for Situational Analysis and Design Methods
www.irma-international.org/chapter/meta-modeling-situational-analysis-design/21060/

E-CARe: A Process for Engineering Ubiquitous Information Systems
www.irma-international.org/article/e-care/80194/

Threat Analysis in Goal-Oriented Security Requirements Modelling
www.irma-international.org/article/threat-analysis-in-goal-oriented-security-requirements-modelling/113724/

Security Gaps in Databases: A Comparison of Alternative Software Products for Web Applications Support
www.irma-international.org/article/security-gaps-databases/58507/

Specifying Knowledge Graph with Data Graph, Information Graph, Knowledge Graph, and Wisdom Graph
www.irma-international.org/article/specifying-knowledge-graph-with-data-graph-information-graph-knowledge-graph-and-wisdom-graph/201482/