Modeling the Impact of Biometric Security on Millennials’ Protection Motivation

Benjamin Ngugi, Suffolk University, Boston, MA, USA
Arnold Kamis, Suffolk University, Boston, MA, USA

ABSTRACT

Security researchers and managers would like to know the best ways of introducing new innovations and motivating their use. This study applies Protection Motivation Theory to model the coping and threat appraisals that motivate Millennials, who are early technology adopters, to adopt or resist biometric security for system access. One hundred fifty-nine Millennials were given a hypothetical scenario in which system access would be enhanced by biometric security to strengthen user authentication. The authors model the results with PLS and find that Protection Motivation Theory provides a good explanation of the user’s perceptions of biometric security. The model suggests that the users’ protection motivation is influenced directly by the Perceived System Response Efficacy of the biometric system and indirectly by Perceived Effort Expectancy, Perceived Computer Self-Efficacy, Perceived Privacy Invasion and Perceived System Vulnerability. Implications and limitations of the model are discussed.

Keywords: Authentication, Biometric Security, Coping and Threat Appraisals, Effort Expectancy, Perceived Computer Self-Efficacy, Privacy Invasion, Protection Motivation Theory, System Vulnerability

1. INTRODUCTION

The number of computer breaches and the resulting disclosure of personal identifying information is on the increase (Identity Theft Resource Center, 2010). Such information is used to create counterfeit cards and identification documents (Balanoiu, 2009). Identity thieves can masquerade as authentic users and charge counterfeit credit cards to the maximum. The fact that an impostor can masquerade as the authentic user simply because he or she possesses a counterfeit card and a stolen PIN is a manifestation of the weaknesses of current authentication systems.

One way of making authentication systems stronger and more reliable is to add a biometric layer on top of current security controls. A system designer can choose from two broad categories of biometric technology. One option is to add a physical biometric, which relies upon some unique physical characteristic, e.g. a fingerprint biometric. Another option is to leverage behavioral biometrics, which depend
on user behavioral patterns, e.g., a typing-pattern generated by the user’s typing of his name and password. Physical biometric technology, e.g., the fingerprint biometric, is more accurate than behavioral biometric technology, e.g., the typing-pattern biometric, but may not be appropriate because of higher costs or privacy invasion (National Center for State Courts, 2002). Further, a behavioral biometric technology could exploit the advantages of ubiquitous technology, e.g., computer keyboards, numeric keypads, or keyless door entry systems. In either category of biometric technology, an extra layer of technology can enhance security because it is difficult to provide correct biometric credentials unless one is the authentic person. In this paper, we choose to test the typing-pattern biometric as a low-cost, minimally intrusive example of behavioral biometrics. The overall biometric technology market is expected to grow to $9.4M in 2014 (International Biometric Group, 2010).

Biometric technology can be expensive to purchase and objectionable to users, however, because of a feeling of invasiveness. The organization buying such technology must make significant investments in time and money to install such systems and train end users. In addition, the use of such technology comes with several costs to the user. For example, the user spends time and effort to input his or her biometric patterns during enrollment to provide the biometric features signature, which can be compared with future log-in patterns during verification. The user also must go through all the steps at every system login to provide a new biometric pattern for comparison with the stored biometric template.

By agreeing to give their personal biometric patterns, users are potentially giving up some privacy and making themselves vulnerable to unauthorized use of their patterns. Security managers wrestle with several questions and tradeoffs. They have to consider the best way of motivating users to consider the new technology with a receptive attitude. This is because previous work has demonstrated that a user’s “attitude toward a technology has significant, positive effect on the technology usage behavior” (Chau, 2001). Security managers will have to estimate the utility that the user derives from the new technology and how much they are willing to do before they feel that the benefits are not worth the effort. Management would also like to know if there are factors that would moderate this effort in one direction or the other.

There is currently little research that addresses the gap at the intersection of technology protection motivation and biometric engineering. This paper addresses that gap by investigating the coping and threat appraisals that influence user protection motivation to use a behavioral biometric technology. Our contribution is a model of protection motivation at the individual unit of analysis in the context of voluntary use of biometric technology. For example, if a bank were to implement biometric-enabled ATM machines and allow users the option of enrolling for advanced authentication by registering their biometric patterns. Users will have the freedom of not enrolling and simply continuing to use the existing PIN and ATM card authentication system. Additionally the user can opt to close her account and easily switch to another bank that does not implement biometric authentication at all.

We start by reviewing previous work and then propose several hypotheses and a research model as the foundation for the rest of the investigation. We then review our methods and show the validated statistical model.

2. RESEARCH FRAMEWORK AND MODEL DEVELOPMENT

Researchers in the field of technology acceptance have identified various factors that are important in the acceptance of new technologies (Davis, 1989; Ma & Liu, 2004; Venkatesh, Morris, Davis, & Davis, 2003). However, there is a need for further research on the critical factors that would motivate users to protect themselves with biometric technologies.

We reviewed several theories and selected Protection Motivation Theory (PMT) as the most appropriate for modeling the protection motivation with biometric technology. PMT is based on Theory of Planned Behavior (Ander-
Protective Measures and Security Policy Non-Compliance Intention: IT Vision Conflict as a Moderator
www.igi-global.com/article/protective-measures-and-security-policy-non-compliance-intention/216969?camid=4v1a

Exploring Online Transaction Self-Efficacy in Trust Building in B2C E-Commerce
www.igi-global.com/article/exploring-online-transaction-self-efficacy/3851?camid=4v1a

Studying the Documentation of an API for Enterprise Service-Oriented Architecture
Brad A. Myers, Sae Young Jeong, Yingyu Xie, Jack Beaton, Jeff Stylos, Ralf Ehret, Jan Karstens, Arkin Efeoglu and Daniela K. Busse (2010). Journal of Organizational and End User Computing (pp. 23-51).
www.igi-global.com/article/studying-documentation-api-enterprise-service/39119?camid=4v1a