Decision Support Systems 51 (2011) 394–404

Contents lists available at ScienceDirect

Decision Support Systems

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

Cost and benefit analysis of authentication systems

Kemal Altinkemer [a,*], Tawei Wang [b,*]

[a] Krannert Graduate School of Management, Purdue University, 403 W. State Street, West Lafayette, IN 47907, United States
[b] Department and Graduate Institute of Accounting, College of Management, National Taiwan University, Taipei, 106 Taiwan

ARTICLE INFO

Article history:
Received 10 April 2009
Received in revised form 10 January 2011
Accepted 20 January 2011
Available online 31 January 2011

Keywords:
Information security
Authentication
Biometric
Two-factor authentication

ABSTRACT

This study investigates the key elements an online service or product provider needs to consider when adopting another single-factor or two-factor authentication system. We also uncover the conditions that make the new one-factor or two-factor authentication system more preferable. By using the probability of system failure, this study generalizes all possible combination of authentication systems into four different cases. This generalization allows us to compare different systems and to determine the key factors managers need to consider when adopting a new authentication system. The key factors are (1) additional implementation costs, (2) customer switching which is determined by the market share and customers' preferences, and (3) expected losses when the new system fails. This study also suggests that if the provider chooses an expensive new system, the provider needs to have a larger market share to justify the spending. Also, regulators can encourage the adoption of a more secure authentication system by changing the penalty a firm faces when the system fails. Finally, it could also be preferable to have both one-factor and two-factor authentication systems depending on the customers' characteristics.

1. Introduction

Authentication can be used to verify either the content of the message, the origin of the message, or the identity of the user [26,41]. Identity authentication focuses on the process of verifying a person's identity. In general, the information (or factors) people use to identify themselves is (1) something the user is. This is biometric information, such as fingerprints; (2) something the user has, such as an ID card; (3) something the user knows, such as a password [30]. In some situations, users have to provide two of the above information simultaneously, for instance, an Automatic Teller Machine (ATM) card and a Personal Identification Number (PIN). This is called two-factor authentication. Two-factor or multi-factor authentication, as the name suggests, uses more than one single piece of information when granting access right. By using more information, the authentication system could be more secure (e.g., [45]). Given that the new authentication system could be more secure and as the concerns about identity theft have increased its popularity [4], people start to propose the use of two-factor authentication systems in order to effectively distinguish imposters from genuine users. For example, the Federal Financial Institutions Examination Council (FFIEC) released guidance on authentication in Internet banking environment on October 12, 2005 [16]. This guidance asked all the regulated agencies, by the end of 2006, to conduct risk-based assessments and to develop security measures to reliably authenticate (i.e., two-factor or multi-factor authentication) customers remotely accessing their online financial services.

A multi-factor authentication system seems to be more secure but the firm might need to allocate more resources on implementations, such as software, hardware, and training [45]. From the customers' viewpoint, multi-factor authentication could be accompanied with the concerns about the use of additional information collected. The new interfaces, new devices, and the new authentication processes could also result in inconvenience of the new authentication system and a prolonged time needed to complete the transaction. All of the above issues could at the same time affect an online service or product provider's decision when implementing a new authentication system.

This paper focuses on the decision of implementing a new authentication system and addresses the following research questions. First, from an online service or product provider's perspective, what are the key elements it needs to consider when adopting another single-factor or two-factor authentication system? Second, what are the conditions that make the new one-factor or two-factor authentication system more preferable? Given that there are all kinds of authentication technologies, it is unrealistic to compare different authentication methods or to optimize the decision by considering all the possibilities. Therefore, in order to answer our research questions, we use a static model as a first attempt to understand the decision of choosing authentication systems. In particular, this study first generalizes all the authentication systems into two broad types. Based on the generalization, we compare the conditions that make the new authentication system more preferable regardless of the detail

* Corresponding authors.
E-mail addresses: kemal@purdue.edu (K. Altinkemer), twang@ntu.edu.tw (T. Wang).

0167-9236/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2011.01.005

specification of the technology. These conditions allow us to uncover the rules that provide rationale for managers to choose authentication systems.

The remaining of the paper is organized as follows. Relevant literature on authentication and privacy are reviewed in Section 2. In Section 3, we propose a static model for one-factor and two-factor authentication systems. This model leads to our propositions and managerial implications in Section 4. We conclude with contributions, and possible avenues for future research in Section 5.

2. Literature review

There are two major streams of literature related to our research: authentication, and privacy in the context of authentication systems and privacy from an economic perspective.

2.1. Authentication

The literature on authentication has long been discussed from the technical perspective. For instance, Woo and Lam [46] and Diffle et al. [15] provide the basic authentication mechanisms and the goals of authentication. Other studies focus on the design of protocols (e.g., [1,40]) or ways to implement or improve authentication methods (e.g., [5,6,37]). However, studies about authentication from an economic perspective are limited. These studies are often embedded in the discussion of other issues. For example, Anderson [3] discusses the role of authentication in information security from an economic perspective. Also, authentication has also been discussed in internal control, EDP auditing, assurance, knowledge sharing as well as group decision literature (e.g., [19,27,39,42]). Different from previous literature, our study formally focuses on the authentication system decisions from an economic perspective and provides decision rules for managers.

2.2. Privacy in the context of authentication systems and privacy from an economic perspective

It is unavoidable to obtain users' personal identifiable information when implementing an authentication system, such as names, addresses, purchasing history, or biometric images of an individual (e.g., [29,34]). Several studies have discussed the collection of personal identifiable information and the techniques to preserve privacy in the context of authentication systems (e.g., [6,10,13,14,32]). Accordingly, this study also relates to, though not directly, the literature on privacy from an economic perspective. Privacy is defined as the individual's ability to control the collection and use of personal information (e.g., [18,21,24,36,44]). Studies about privacy from an economic perspective include reviews on the economic analyses of privacy (e.g., [24]), how businesses use personal information to customize services and to discriminate consumers (e.g., [12,20,47]), and how business use personal information for promotions and cross market information (e.g., [2,22]). The violation of privacy depends on (1) whether consumers can control the amount and the depth of information collected, and (2) the knowledge of the collection and use of their personal information [11]. For instance, Hoffman et al. [23] show that about 95% of online users are reluctant to provide personal information to websites because of privacy concerns. In the context of authentication systems, the change in authentication level could imply the need for more information depending on the system a firm chooses and the amount of information that might lose once the system fails. The privacy concerns about providing personal identifiable information could affect customers' willingness to use an authentication system which in turn affects a firm's decision on authentication systems. Therefore, the privacy concerns are involved in the selection process of authentication system alternatives.

3. Model

In this section, we first present the basic settings for our analysis. Then the definition and the probability of system failure under different authentication methods are discussed followed by the details of our models for one-factor and two-factor authentication systems. Finally, by comparing the expected costs and losses associated with different authentication systems, we show the conditions that make the new authentication system preferable.

3.1. Basic settings

We focus on one online service or product provider in this study. This provider currently has a market share of m in the service or product category it provides, where $0<m<1$ (see Appendix A for variable definitions). This market share m can also be interpreted as the total value the provider can get from the customers compared to other providers. In order to complete the transaction process, each of the providers' customers is required to provide a certain level (α, $0<\alpha\leq 1$) of personal information, such as name, address, and phone number. If the system fails, the product or service provider might need to compensate its consumers' losses and to pay a legal penalty or fine (L for both the compensation and penalties) for not abiding by the privacy commitment or regulations (e.g., [38]). The compensation of customers' losses and the penalties (L) increases as the number of customers that are affected (i.e., m) and the level of information the customers provide (i.e., α) increase.

The customers are categorized along two dimensions: privacy and convenience. The first dimension is privacy sensitivity. A proportion of customers (ρ, $0\leq\rho\leq 1$) are privacy sensitive in the market the provider faces. This portion of customers has more concerns about the information collected from them and the use of such information. Therefore, adopting another authentication system, a provider might attract some potential customers and lose some existing customers both because of the privacy concerns. The new system might protect the information better (e.g., [45]) and attract some potential customers. However, when the new system is breached, more information could be lost and some of the existing customers might choose not to continue subscribing or purchasing from the provider.

The second dimension is convenience sensitivity. A proportion of customers (δ, $0\leq\delta\leq 1$) emphasize more on the convenience of the transaction such as the new interface and the new processes. After the provider switches to a new authentication system, the provider might lose a certain portion of existing customers because of the possible inconvenience, such as prolonged transaction time, caused by the new system. This categorization is illustrated in Table 1.

In this paper, system failure is defined as any situation in which non-genuine users (e.g., hackers) are able to access to the information or genuine users are unable to access to the information because of the failure of the software or hardware, compatibility issue of the software or hardware, for example, or the successful action of the hackers. Based on the definition, we discuss the probability of system failure for different authentication systems.

3.2. Probability of system failure

We group all the authentication systems into three categories as mentioned in the Introduction, namely, (1) something the user has,

Table 1
The categorization of customers.

Privacy sensitivity	High	$\rho(1\text{-}\delta)$	$\rho\delta$
	Low	$(1\text{-}\rho)$ $(1\text{-}\delta)$	$(1\text{-}\rho)\delta$
		Low	High
		Convenience Sensitivity	