Available online at www.sciencedirect.com

SCIENCE DIRECT®

Decision Support Systems 41 (2005) 242–261

Decision Support Systems

www.elsevier.com/locate/dsw

Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis

G.B. Tanna[a], M. Gupta[a], H.R. Rao[b,*], S. Upadhyaya[c]

[a]*M&T Bank, United States*
[b]*MSS Department, School of Management, SUNY Buffalo, United States*
[c]*CSE Department, College of Engineering, SUNY Buffalo, United States*

Received 31 August 2003; received in revised form 30 June 2004; accepted 30 June 2004
Available online 1 September 2004

Abstract

One of the fastest growing applications in the banking arena is Electronic Bill Presentation and Payment (EBPP), driven primarily by a desire to reduce costs associated with issuing and settling physical bills. EBPP is a secure system for companies to electronically present bills and other related information to their customers, and host the secure payment of these bills. This paper puts forth information assurance issues that are analyzed from a workflow and transaction analysis perspective. Various aspects and technologies deployed in EBPP systems are discussed with a view to understand security underpinnings. The paper develops a framework for the measurement of security levels of any EBPP system, which will help security personnel to ensure a higher level of understanding of information assurance issues and proactively engage in elevating security measures and fraud protection in their organizations. A step-by-step procedure is developed to help IT security managers and administrators to understand the metrics that can define proactive and reactive security service delivery levels, and implement the measurement framework that is necessary to demonstrate performance against these metrics.

Keywords: EBPP systems; Electronic payment and presentation; Information assurance; Security measurement; Security metrics; Threat analysis; Workflow analysis

1. Introduction

Advances in telecommunications and information technologies are leading to a revolution in the payment industry in the banking arena. With the rise in the use of Internet for carrying out operations and

* Corresponding author. Tel.: +1 716 636 8866; fax: +1 716 636 6117.
E-mail address: mgmtrao@buffalo.edu (H.R. Rao).

0167-9236/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2004.06.013

functions that were traditionally done through paper, pen and snail-mail, with the help of electronic systems, the importance of Electronic Bill Presentation and Payment (EBPP) cannot be over-emphasized. So, although paper-checks are still the dominant way of making payments [5], EBPP is a modern and convenient form of making payments with the expediency of instant confirmation and faster postings of those payments [6].

Notably, there are a couple of payment services models: (1) The Biller-Centric Model or the Direct Model, and (2) The Payer-Centric Model or the Consolidator Model. However, the value proposition inherent in payer-centric systems is more balanced than the traditional method of posting invoices on billers' websites. Biller-centric solutions put the burden on the payer to visit multiple sites for their invoices, and there is little incentive for payers—particularly large organizations—to want to do this [7].

In this paper, we focus our attention on the payer-centric model. This model of the bill-payment process involves five parties or entities. They are: (1) Consumer, (2) Consumer's Financial Institution, (3) Biller, (4) Biller's Financial Institution and (5) The Payment Network. A typical flow of information between the five parties/entities involved is depicted in Fig. 1.

The model presented in the paper can aid IS managers to understand their organization's IS posture and manage IS risks by taking proactive measures rather than reactive ones. The contribution of the paper is twofold—it develops (1) detailed transactional workflows that can be used to expose the vulnerabilities that are prevalent in the electronic bill-payment system using a comprehensive threat analysis model (details of which are discussed in a later section) to conduct a systematic threat analysis; (2) a framework and a step-by-step procedure to help IT security managers and administrators to develop a vulnerability score to understand the metrics that can define proactive and reactive security service delivery levels, and implement the measurement capability that is necessary to demonstrate performance against these metrics. This can serve as launching pad for risk assessment of EBPP or similar systems. Since, some parts of the model are based on subjective evaluations of risk factors, experience of the reviewer, and biased outlook towards the environment, etc., would come into play. Even so, the framework presented here can be adapted to the environment and be refined subsequent to feedback-based iterative corrections. The score thus derived can serve as baseline for assessing the strength of a system's security posture with time and improvements.

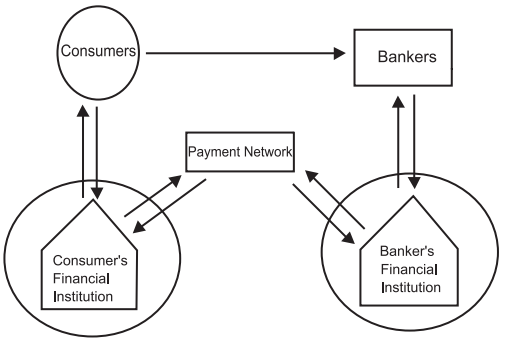

Fig. 1. A typical information flow for a bill-payment system [1].

The rest of the paper is organized as follows. Section 2 discusses the technologies and components of the EBPP systems. A detailed analysis of the architecture is also carried to examine information assurance issues in the links. Section 3 presents a state diagram and transaction analysis of EBPP systems with respect to security issues. Then we present an extension of the STRIDE[1] threat analysis model and its detailed adaptation with the EBPP system in Section 4. Section 5 outlays threat identification and analysis of EBPP system vis-à-vis the adapted STRIDE Model. Identification and measurement of security of the system is carried out through the transaction workflow analysis of the EBPP system. Finally, a framework, based on workflow states, to derive an overall vulnerability score for the EBPP system is developed in Section 6. This security measurement framework will help IT security managers and administrators gauge the security posture of the EBPP system and proactively engage in remediation of the weaknesses and IS risk mitigation in general.

[1] Developed by Microsoft, the STRIDE Model gets its name from the first letter of the threat categories identified by them, e.g., S=Spoofing Identity, T=Tampering of Data and so on.)