Chapter VII

Stronger Authentication: Responding to the Crisis of Confidence

Alvin Y. C. Yeo, SIM University, Singapore

Abstract

Authentication is a prime challenge for banks today as end users’ digital identities are being compromised through increasingly sophisticated means. This chapter provides a timely review of the authentication concept and key authentication technologies, namely password tokens, biometrics, smart cards, smart tokens, and out-of-band authentication. An integrative model is proposed, which frames three key considerations in choosing an authentication solution—cyber threat types, regulatory requirements, and business considerations. Each of the implications is considered in turn. Finally, to guide future deployments of authentication solutions, the chapter concludes with pragmatic suggestions by proposing a set of evaluation criteria for choosing authentication solutions and key legal considerations.

Copyright © 2008, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Introduction

The use of infocomm technology is pervasive in today’s wired world. Mainstream consumer services, such as health care and education, are migrating online. In the banking sector, this process has been going on for some years, beginning with automated teller machines (ATMs) and over, the past decade or so, telephone banking and personal computer (PC)-based proprietary systems. The Internet significantly expanded the banks’ distribution scope, no doubt catalyzed by the fact that an Internet bank user is substantially cheaper to serve than a branch bank customer is.

However, the extent and maliciousness of cyber threats steadily have been escalating, in tandem with the evolving infrastructure landscape. With ubiquitous connectivity, data, such as bank account numbers and credit card details, may be available on networks. If someone can steal such vital identity-related information, that person may be able to access another’s bank account or credit information. This makes online bank users prime targets.

Lured by high profits and low risks, organized crime syndicates are quickly replacing casual hackers in perpetrating acts like cyber espionage, cyber extortions, and identity thefts. End users, who previously were not prime targets, have become targets of opportunity, when their security posture is not maintained.

In particular, identity theft is flourishing, and one easy and increasingly popular way of capturing personal data is called “phishing” (Lepofsky, 2004). This scam involves e-mail messages that purportedly come from legitimate businesses (e.g., ABN Amro, Citibank), asking for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. In particular, the Anti-Phishing Working Group found that 85% of the 14,000 unique phishing attacks in August 2005 were directed against customers of financial institutions (Marlin, 2005). This places an increasing importance and burden on authentication mechanisms and banks for validating those identities.

These phenomena, perpetuated in stealth, undermines consumer confidence in online services and, at the same time, deters the innovation of value-added services by banks. Lee and Turban (2001) argue that the lack of trust is increasingly a key impediment to the growth of Internet banking. According to a survey conducted by market research firm Gartner of 5,000 U.S. Internet users, 28% of the respondents said concerns about cyber attacks have affected their online banking behavior; 14% have stopped paying bills via online banking; and about 4% have completely given up on online banking.

The online environment does not allow customers the natural benefits of face-to-face communications (Ba, Whinston, & Zhang, 1999; Citera, Beauregard, & Mitsuya, 2005). This temporal and spatial separation increases fears of opportunism arising from product and identity uncertainty. As Dellarocas (2001) noted, “...the more the two sides of a transaction are separated in time and space, the greater the risks” (p. 2). Overall, these unique differences decrease customers’ perceptions of control over their online transactions and erode consumer confidence in online banking.

Financial regulators worldwide are responding to these challenges. For example, in the United States, the Federal Financial Institutions Examination Council (FFIEC) has given banks until the end of 2006 to implement two-factor authentication, which relies on something the consumer has, such as hardware tokens or smart cards, as well as something the
The Problems of Stage Acquisition Under the New Consolidation Accounting Standards
www.igi-global.com/article/the-problems-of-stage-acquisition-under-the-new-consolidation-accounting-standards/193900?camid=4v1a