Chapter XIX
Security of Alternative Delivery Channels in Banking: Issues and Countermeasures

Manish Gupta
State University of New York, USA

H. Raghav Rao
State University of New York, USA

Shambhu Upadhyaya
State University of New York, USA

ABSTRACT

To sustain competitive advantages, financial institutions continuously strive to innovate and offer new banking channels to their customers as technology creates new dimensions to their banking systems. One of the most popular such diversification of channel is electronic banking (e-banking). Information assurance is a key component in e-banking services. This chapter investigates the information assurance issues and tenets of e-banking security that would be needed for design, development and assessment of an adequate electronic security infrastructure. The technology terminology and frameworks presented in the chapter are with the view to equip the reader with a glimpse of the state-of-art technologies that may help towards learned and better decisions regarding electronic security.

INTRODUCTION

The Internet has emerged as the dominant medium in enabling banking transactions. Adoption of e-Banking has witnessed an unprecedented increase over the last few years. Twenty per cent of Internet users now access online banking services, a total that will reach 33 per cent by 2006, according to

The Online Banking Report. By 2010, over 55 million US households will use online banking and e-Payments services, which are tipped as "growth areas". The popularity of online banking is projected to grow from 22 million households in 2002 to 34 million in 2005, according to Financial Insite, publisher of the Online Banking Report newsletter. Developing alternative channels for retaining customers as well as for attracting new ones is very important to financial institutions (Kimball & Gregor, 1995; Thornton & White, 2001). For this reason, financial institutions offer new banking channels to their customers, as the technology adds new dimensions to the classic banking systems (Eriksson & Nilsson, 2007). For example, over the last few years, self-service technologies have replaced the need for face-to-face interaction between banks and customers (Eriksson & Nilsson, 2007).

Electronic banking uses computer and electronic technology as a substitute for checks and other paper transactions. E-Banking is initiated through devices such as cards or codes to gain access to an account. Many financial institutions use an automated teller machine (ATM) card and a personal identification number (PIN) for this purpose. Others use home banking, which involves installing a thick client on a home PC and using a secure dial-up network to access account information and still others allow banking via the Internet. In industrialized countries, the use of electronic channels to manage one's wealth has increased. From the customers' perspective, electronic payments instruments and channels have made money impersonal and virtual (Singh, 2004). In a survey of e-banking customers, 76% persons without disability with a household income above $50,000 said they used Internet banking (Singh et al, 2009).

This chapter will discuss the information assurance issues (Maconachy, et.al , 2002) that are associated with e-banking infrastructure. We hope that the chapter will allow IT managers to understand information assurance issues in e-banking in a holistic manner, and help them make recommendations and actions to ensure security of e-banking components.

INTERNET/WEB BANKING

A customer links to the Internet from his PC. The Internet connection is made through a public Web server. When the customer brings up the desired bank's Web page, he goes through the front-end interface to the bank's Web server, which in turn interfaces with the legacy systems to pull data out for the customer's request. Pulling legacy data is the most difficult part of Web banking. While connection to a Direct Dial Access (DDA) system is fairly straightforward, doing wire transfer transactions or loan applications requires much more sophisticated functionality. A separate e-mail server may be used for customer service requests and other e-mail correspondence. There are also other middleware products that provide security to ensure that the customer's account information is secured, as well as products that convert information into an HTML format. In addition, many of the Internet banking vendors provide consulting services to assist the banks with Web site design and overall architecture. Some systems store financial information and records on client PCs, but use the Internet connections to transmit information from the bank to the customer's PC. For example, the Internet version of Intuit's BankNOW runs offline at the client and connects to the bank via the Internet only to transmit account and transaction information (Walsh, 1999). Although the banking industry has a large capital invested in ATMs, banks are failing to get the desired results (Colonia-Willner, 2004). E-banking services allow customers to remotely, via Internet, manage their bank accounts and transactions (Weir, Anderson, & Jack, 2006). Nowadays, banks provide a complete range of financial services through their Internet banking channels because they are more cost-effective than