Chapter XXII

Implications of FFIEC Guidance on Authentication in Electronic Banking

Manish Gupta
State University of New York, Buffalo, USA

JinKyu Lee
Oklahoma State University, USA

H. R. Rao
State University of New York, Buffalo, USA

ABSTRACT

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. In today’s online financial services environment, authentication is the bedrock of information security. Simple password authentication is the prevailing paradigm, but its weaknesses are all too evident in today’s context. In order to address the nature of similar vulnerabilities, in October 2005, the Federal Financial Institutions Examination Council (FFIEC)—which comprises the United States’ five federal banking regulators—published joint guidance entitled Authentication in an Internet Banking Environment, recommending that financial institutions deploy security measures to reliably authenticate their online banking customers. The analysis of FFIEC guidance presented in the article are with the view to equip the reader with a glimpse of the issues involved in understanding the guidance for specific banking organization that may help towards learned and better decisions regarding compliance and improved security. The chapter will allow Information Technology 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.

INTRODUCTION AND BACKGROUND

The Internet is an integral part of our daily lives, and the proportion of people who expect to be able to manage their bank accounts anywhere, anytime is constantly growing and Internet banking has come of age as a crucial component of any financial institution’s multichannel strategy (Hiltgen et al., 2006). Information about financial institutions, their customers, and their transactions is, by necessity, extremely sensitive; thus, doing such business via a public network introduces
new challenges for security and trustworthiness (Hiltgen, Kramp, & Weigold, 2006). Adoption of e-banking has witnessed an unprecedented increase over the last few years. 20% of Internet users now access online banking services, a total that will reach 33% by 2006, according to the Online Banking Report (Gupta, Rao, & Upadhyaya, 2004). By 2010, over 55 million U.S. households will use online banking and e-payments services, which are tipped as “growth areas.” Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and nonrepudiation, which means it must ensure that only qualified people can access an Internet banking account, that the information viewed remains private and cannot be modified by third parties, and that any transactions made are traceable and verifiable (Hiltgen et al., 2006).

INTERNET BANKING AND AUTHENTICATION

The actual and perceived threats to Internet-based banking define the need for a set of interrelated security services to provide protection to all parties that can benefit from Web banking in a secure environment (Gupta et al., 2004). The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

Security for financial transactions is of vital importance to financial institutions providing or planning to provide service delivery to customers over the public Internet, as well as to suppliers of products, services, and solutions for Internet based e-commerce. With security incidents such as identity theft and account hijacking undermining customer confidence, slowing adoption rates and threatening profits, it is very evident that requirement to go beyond mere passwords for authentication is real and important. The recent FFIEC guidance on authentication in online banking reports “Account fraud and identity theft are frequently the result of single factor (e.g., ID/password) authentication exploitation” (FFIEC, 2005).

In today’s online financial services environment, authentication is the bedrock of information security. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today’s Web. Password reuse, insecure passwords, and poor password management practices open a world of attacks by themselves (Jones, 2006). It is high time for financial institutions re-evaluate authentication strategy, in light of the fact that cyber attacks are only going to grow in sophistication and in impact.

CHAPTER ORGANIZATION AND CONTRIBUTION

The chapter discusses impact and issues surrounding FFIEC guidelines for stronger authentication requirements for online banking. The chapter analyses the opportunities and costs of initiatives that financial institutions have to undertake to comply by these guidelines. First the chapter discusses implications, requirements, and risks involved with the authentication guideline and how they interact with one another in determination of an execution plan. This encompasses the assessment phase of the guidance evaluation. Then, the chapter discusses various state-of-art authentication technologies, processes, and methods that can be reviewed and investigated further for their appropriateness in a specific organizational and business context. This is the compliance and implementation phase. Here, the chapter demonstrates how components of assessment phase interact with compliance and implementation phase. Figure 1 illustrates the architecture of the guidance evaluation methodology and interactions amongst its components. The chapter concludes with commentary on the analyses and recommendations.

THE FFIEC GUIDANCE

The Federal Financial Institutions Examination Council (FFIEC) is an interagency council set up to develop standards for the federal auditing of financial institutions by bodies such as the Federal Reserve System and the Federal Deposit Insurance Corp. (FDIC). In October 2005, the Federal Financial Institutions Examination Council (FFIEC)—which comprises the United States’ five federal banking regulators—published joint guidance entitled Authentication in an Internet Banking Environment, recommending that financial institutions deploy security measures to reliably authenticate their online banking customers. The new guidelines are not a law, but are more like best practices that banks will be audited against.
Related Content

Windows Essentials Before We Start
(2019). Constructing an Ethical Hacking Knowledge Base for Threat Awareness and Prevention (pp. 72-105).
www.igi-global.com/chapter/windows-essentials-before-we-start/218415?camid=4v1a

A Mark-Up Language for the Specification of Information Security Governance Requirements
www.igi-global.com/article/mark-language-specification-information-security/55378?camid=4v1a


Architectures for Advanced Cryptographic Systems
www.igi-global.com/chapter/architectures-advanced-cryptographic-systems/23127?camid=4v1a