Chapter VI

New Technologies in E-Banking: Convenient and Trustworthy?

Niels Jørgensen, Roskilde University, Denmark

Abstract

In e-banking, user authentication with mobile phones and special-purpose cryptographic tokens is a promising alternative to conventional approaches, such as digital signatures on a personal computer (PC). Special-purpose tokens that do not have external connections avoid viruses transmitted via the Internet. Moreover, phones and tokens are mobile. The chapter assesses the potential of new technologies for user authentication (verification of the user’s identity) on the basis of a practical test and an analysis of trust. The practical test comprises a password generator, mobile phones with short message service (SMS), wireless application protocol (WAP), and third generation (3G), and (conventional) PC-based authentication, using digital signatures—all as used by a Danish e-bank. On the one hand, the test indicates that in some ways the hardware-based technologies are indeed easier to use. On the other hand, the trust analysis indicates that the secrecy of the new approaches may be a weakness, since there is no publicly available analysis of their security. The secrecy of the hardware-based technologies may be justified by the need to prevent various attacks, such as physically opening a password generator to determine its secret key. A prerequisite for consumer trust in the hardware-based technologies may be the introduction of security evaluation methods that do not disclose the secret parts of the technologies to the public and are conducted by public authorities or independent third parties.
Introduction

A dilemma is facing systems for Web-based electronic banking (e-banking). E-banking must be secure and easy to use, but the two goals are in conflict. Passwords provide an illustration of the dilemma. On the one hand, a strong password such as x7h%r%C9 is less vulnerable to attack than a simple password, such as a person name. On the other hand, a strong password may be difficult to remember, so the user is tempted to write the password on paper attached to the computer screen. The dilemma of passwords is widely acknowledged (Morris & Thomson, 1979; Schultz, Proctor, Lien, & Salvendy, 2001).

Digital signatures provide much better security than passwords but do not solve the basic conflict between security and ease of use. In their best practice recommendations, Claessens, Dem, De Cock, Preneel, & Vandewalle (2002) noted that in principle, digital signatures are the most secure method for authentication, but when stored on a user’s PC, a signature file requires the user to protect the PC against intrusion from the Internet, which requires skills and time. Therefore special-purpose cryptographic hardware tokens were recommended as a best practice.

A recent event in Denmark highlights the risks of storing digital signatures on Internet-connected computers. In 2004, a person stole 25,000 DKR (approximately $4,000 (US)) from a private e-bank account in Nordea, which holds the second largest market share in Denmark. The attacker managed to transfer, via the Internet, a Trojan-horse program to the account holder’s computer. The program obtained the signature file and the password and transmitted them to the attacker’s computer. The signature file was copied from the hard disk, and the password was intercepted when the user typed it on the keyboard. In this case, the attacker was caught easily, since he transferred money from the victim’s account to his own (RB-Børsen, 2004).

E-banking is widely used in Denmark. In 2006, 83% of the population had access to the Internet from home, and in a given month, 56% of the population had logged on to a private e-banking account (Danmarks Statistik, 2006). Recently, several Danish banks have introduced alternatives to digital signatures. These are a password generator called ActivCard® and GSM mobile phones with SMS, WAP, or 3G. This provided the opportunity to conduct the practical test of the new technologies that is reported in this chapter.

Picture 1. Hardware tokens of the test: From left are a 3g mobile phone (Nokia 6680), a password generator (ActivCard®), and a 2g mobile phone (Nokia 7650)
Related Content

The Impact of Firm Specific Factors on Capital Structure: Empirical Evidence from Turkey
[www.igi-global.com/article/the-impact-of-firm-specific-factors-on-capital-structure/119399?camid=4v1a](www.igi-global.com/article/the-impact-of-firm-specific-factors-on-capital-structure/119399?camid=4v1a)

The Impact of Ownership Structure on Firm Performance: Evidence from Pakistan
[www.igi-global.com/article/the-impact-of-ownership-structure-on-firm-performance/164986?camid=4v1a](www.igi-global.com/article/the-impact-of-ownership-structure-on-firm-performance/164986?camid=4v1a)

CLS Bank
[www.igi-global.com/chapter/cls-bank/54705?camid=4v1a](www.igi-global.com/chapter/cls-bank/54705?camid=4v1a)
Emerging Auditing Perspectives in the Age of the Fourth Industrial Revolution
[www.igi-global.com/chapter/emerging-auditing-perspectives-in-the-age-of-the-fourth-industrial-revolution/222625?camid=4v1a](www.igi-global.com/chapter/emerging-auditing-perspectives-in-the-age-of-the-fourth-industrial-revolution/222625?camid=4v1a)