Chapter XXXVI
Mobility for Secure Multi-Factor "Out of Band" Authentication

Matthew Tatham
Alacrity Technologies, Australia

Arsi Honkanen
Alacrity Technologies, Australia

ABSTRACT

Securing data is a key concern for individuals and organisations throughout the world, especially within information and communications infrastructure. With the help of highly sensitive data such as individual account information, criminals can carry out a variety of fraudulent activities; most notably financial fraud, which can be carried out through a multitude of channels. The increasing utilization of technologies, devices, and processes has further exacerbated these risks to organisations. This chapter identifies and describes the issues surrounding the secure authentication of individuals attempting to access or transact with organisations using online networks. This chapter then explains how to secure access to sensitive data through the use of multi-factor out-of-band authentication.

INTRODUCTION

Security is of major concern to organisations across the globe. As Nand (2006) stated, issues of security are a particularly significant and critical success factor in mobile business. This is the case since, although wireless connectivity offers portability and hence mobility - it adds to the risk of unauthorised access to the system and data disclosure. Guarding access to sensitive data, particularly in large government organisations and financial institutions, is becoming increasingly important to the overall security strategy for organisations. According to Dunn (2006):

"Global crime is now one of the three big issues facing the world, the other two being political violence and climate change. Of course, if you were sitting in an air-conditioned office insulated by layers of security guards, this might not have dawned on you. But it will, one day."

The flexibility and cost effective nature of the Internet, as a vehicle for communicating as well as processing data has allowed organisations and individuals to consider utilising the Internet more than ever before. Utilisation of this method for processing data has also created opportunities for a hacker (who would be interested in gaining unauthorised access to the network). This issue underscores the importance

of securely authenticating legal users of the networks who are attempting to gain access to funds or data.

The risks to the use of the Internet has understandably affected consumer confidence resulting, for many, in a negative perception of this important channel of communication. Society has begun to place pressure on organisations to implement stronger controls to prevent hackers from gaining access to sensitive data. Organisations are required to take responsibility for the protection of customer and employee information.

This chapter discusses practical implementation of stronger security for online authentication activities. The chapter aims to share market research and personal experiences of the authors to assist security managers in examining their current authentication practices as part of an extensive security strategy.

The information in this chapter has been broken down into three distinct segments. The first section of the chapter analyses online banking fraud; cardholder not present (CNP) fraud and data theft; the current tools and methods used by hackers; and the impact this has on organisations and individuals around the world. The second section identifies the various types of authentication solutions available, and the different paths that can be utilised to authenticate an individual for an online transaction. The third section describes the way in which mobility can improve the level of security in the authentication space by utilising a mobile application named Closed Loop Environment for Wireless (CLEW®).

This chapter is written using a combination of the researchers' experiences, along with surveys and statistics used around the world to measure the current state of online fraud and the subsequent effect this type of fraud has on society as a whole. This chapter draws a bridge between mobility and secure authentication through a combination of technologies. Most noteworthy is the use of the mobile device to empower individuals and organisations across the world to prevent unauthorised persons from gaining access to their restricted data.

GROWTH IN ONLINE FRAUD

Fraud, as mentioned in the introduction, is a big challenge in online transactions. However, increasingly it is being combated with the implementation of new controls, such as chip and PIN (Personal Identification Number) for cardholder present transactions. For transactions that utilise the Internet, such as online banking and CNP transactions however, fraud still remains a major concern. There have been a number of articles published regarding the threat of online fraud and the impact this has on society. For example, a BBC article in January, 2007 - "Bank loses $1.1m to online fraud", and the article by Easier Finance "Cyber fraud hitting online retailers hard".

Overall, the cost of online fraud is difficult to determine. This section attempts to analyse some of the hard costs associated with online fraud to consumers, merchants and financial institutions.

Consider, for example, online fraud in Australia. Figures from the Australian Institute of Criminology in 2005 suggest that the total cost of fraud for 2005 in Australia was AU$5 billion. Westpac Banking Corporation (2006) publicly stated that online fraud equates to 6.5% of the total fraud figure. Once these figures were combined, it was determined that, conservatively, the cost of online fraud to Australians is currently AU$325 million, annually.

In the United Kingdom (UK), the UK Payments Association (APACS) stated that online banking fraud increased from £23.2m in 2005 to £33.5m in 2006. This is an increase of 44% year-on-year, and has been driven by an increase in phishing incidents, which went up from 1,713 in 2005 to 14,156 in 2006.

Of the £600 million attributed to credit card fraud for the year 2006 in the UK, £212.6 million was related to CNP transactions. Once again this is recognised as conservative, and CNP fraud is estimated to be increasing at approximately 16% per annum. The introduction of new technologies has reduced all other types of credit card fraud; however CNP fraud is now rising significantly as the fraudsters have moved their attention to the Internet.

In the United States (US), online fraud is still a major issue. The cybercrime forums gird a criminal economy that robs US businesses of $67.2 billion per year, according to a Federal Bureau of Investigations (FBI) projection. Consumer Reports notes that over the past two years US consumers lost more than $8 billion to viruses, spyware and online fraud schemes.

The problem of online fraud is set to increase, with continued use of the current authentication processes. Most authentication processes use the same path for both authentication and the transaction. This use of the same path allows fraudsters to have access to vital information through Trojans and key-logging programs that sit inside many personal computers.