IGI PUBLISHING **ITJ3796**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com

This paper appears in the publication, **International Journal of Information Security and Privacy**, Volume 1, Issue 3
edited by **Hamid R. Nemati © 2007, IGI Global**

A Rule-Based and Game-Theoretic Approach to Online Credit Card Fraud Detection

Vishal Vatsa, Indian Institute of Technology, India
Shamik Sural, Indian Institute of Technology, India
A. K. Majumdar, Indian Institute of Technology, India

ABSTRACT

Traditional security mechanisms are often found to be inadequate for protection against attacks by authorized users or intruders posing as authorized users. This has drawn the interest of the research community towards intrusion detection techniques. We model the conflicting motives between an intruder and an intrusion detection system as a multistage game between two players, each trying to maximize its payoff. We consider the specific application of credit card fraud detection and propose a two-tiered architecture having a rule-based component in the first tier and a game-theoretic component in the second tier. Classical game theory is considered useful in many situations because it permits the formulation of strategies that are optimal, regardless of what the adversary does, negating the need for prediction of his/her behavior. However, we use it in a predictive application in the sense that we consider intruders as rational adversaries who would try to behave optimally, and the expected optimal behavior can be determined through game theory.

Keywords: *credit card systems; data mining; electronic commerce; game theory; rule-based system; security*

INTRODUCTION

The popularity of e-commerce applications like online shopping has been growing rapidly over the last several years. According to a recently conducted ACNielsen study, one-tenth of the world's population has now started shopping online (Global Consumer Attitude, 2006). Germany and Great Britain have the largest number of online shoppers and the credit card is the most popular mode of payment (59%). As the number of credit card users is rising

worldwide, opportunity for thieves to steal credit card details and subsequently commit fraud are also increasing. Credit card frauds can be broadly categorized into the following three types:

1. Physical card gets lost or stolen and is used by fraudster.
2. Card number is stolen and used in indirect shopping.
3. Credit card skimming where the data from a card magnetic strip is electronically copied onto another card.

The first type can lead to a huge financial loss as long as the cardholder does not realize the loss of the card immediately. Once the cardholder realizes the loss of the card, the institution issuing the card can cancel it. In the second and the third type of fraud, the cardholder normally realizes the fraudulent transaction on their card after a long period of time. The only way to detect these two types of fraud is to analyze the transaction patterns of the cardholder and find unusual transactions.

Over the last several years, researchers have developed methods to prevent unauthorized access to database applications. All these techniques aim to detect malicious transactions, specifically in databases, but an open problem in this field is to protect the database from well-formed but damaging transactions while limiting the generation of too many false alarms. This assumes significance especially in the domain of e-commerce where a service provider like a credit card company needs to minimize its losses due to fraudulent transactions but, at the same time, does not wish the cardholder to feel hassled too often. If it could confirm all transactions on a credit card with the genuine cardholder, then automated fraud detection would not have been necessary. But this is neither practical nor feasible. Further, there exists a finite possibility of the attacker being able to learn the defense mechanisms in place when involved in repeated attacks on the system. It is imperative that the detection system, in contrast, should be able to learn the strategies of an attacker and adopt a suitable counterstrategy.

Consider intrusion in an e-purchase situation: the fraudster, if in possession of somebody else's credit card details, can attempt a fraudulent transaction over the Internet posing as the genuine cardholder. The fraudster can obtain the credit card details of an unsuspecting cardholder through a number of ways such as shoulder surfing, dumpster diving, packet intercepting, and database stealing (Li & Zhang, 2004). We also add the possibility that unscrupulous employees at merchant establishments, restaurants, gas stations, and so forth, can note down credit card details and possibly pass them on to an organized group of fraudsters. A fraudster aims at deriving the maximum benefit from such a pool of cards either in the short run (by making high-value purchases, even risking detection) or in the long run (by making a number of small-value purchases to avoid obvious detection). The fraud detection system at the credit card company, oblivious of the type of customer it is interacting with, aims at minimizing its loss due to fraudulent transactions through early detection. This can be modeled as two players in a max-min situation, typical of a game-theoretic problem.

The field of game theory has been explored for problems ranging from auctions to chess and its application to the domain of information warfare seems promising. Hamilton, Miller, Ott, and Saydjari (2002a) bring out the possible role of game theory