Chapter 1.19
An Introductory Study on Business Intelligence Security

Chan Gaik Yee
Multimedia University, Malaysia

G. S. V. Radha Krishna Rao
Multimedia University, Malaysia

ABSTRACT

Firstly, the fact that business intelligence (BI) applications are growing in importance, and secondly, the growing and more sophisticated attacks launched by hackers, the concern of how to protect the knowledge capital or databases that come along with BI or in another words, BI security, has thus arisen. In this chapter, the BI environment with its security features is explored, followed by a discussion on intrusion detection (ID) and intrusion prevention (IP) techniques. It is understood through a Web-service case study that it is feasible to have ID and IP as counter-measures to the security threats; thus further enhancing the security of the BI environment or architecture.

INTRODUCTION

Over the years, business intelligence (BI) has evolved to become sets of technically sophisticated but user-friendly tools for efficiently extracting useful and intelligent information from huge volumes of data. This consequently has enabled users who are not so technically inclined to have easy access to the data, analyze them, and draw useful conclusions from them. Basically, what a BI system does is to query a data source (the data source may be from sales and marketing, customers, partners, suppliers, or even competitor related), use data mining techniques to analyze the extracted information, report the results of analysis, and thus enable the users to make timely and accurate decisions. With the rise of e-commerce, more users have become encouraged to utilize BI in the real-time, Web-based world. For instance, an online retailer could make use of BI to analyze data in real time to determine whether

customer purchasing patterns or market conditions have changed For example, if a customer buys more than a certain amount of a product alerted by the BI system, then the online retailer could immediately offer a quantity-based discount to encourage further big purchases.

As BI databases can be centralized in a shared server, it is therefore cost-effective to let hundreds and thousands of users (including mobile users) access the BI database without geographical boundaries. Consequently, more and more organizations see the benefits of utilizing BI and the importance of BI, which is a process of turning data into information and then into knowledge about the customers, competitors, conditions, and economics in the industry, technology, and cultural trends. As a result of this, focus on BI has to be shifted from enhancing the data-warehousing and data-mining techniques such as OLAP (online analytical processing), OLAM (online analytical mining), multidimensional modeling, design methodologies, optimization, indexing, and clustering techniques (Golfarelli, Rizzi, & Cella, 2004; Hu & Cercone, 2002), to how to securely protect these knowledge capitals from being tampered with by unauthorized use.

Another reason why a BI system has to have maximum security is due to the various security threats and malicious attacks that hackers can launch nowadays. Security threats such as denial of service, malicious or virus attack, "Sniffer" attack, "Evil Twins" attack, dictionary attack, and buffer overflow attack, just to name a few, are impossible to be eliminated completely as these attacks can be launched from the interface/perimeter, network, host, or even the application.

Take for example, denial of service attack. It is launched through overwhelming the network connections with massive traffic, usually in the form of fake IP addresses. When the server is full and has reached the maximum capacity with fake connections, the real and authorized users are denied service or access to the network or system.

Attack from another aspect, for example malicious or virus attack, could cripple the computer or operating system by generating malicious programs and at the same time, destroying, deleting, altering files and databases, and so on.

For wired networks, a hacker could make use of a "sniffer," a tool to wiretap or eavesdrop on a computer network; thus grabbing information off the communication line. Even for the wireless, "Evil Twins" could disguise as hot spots; thus stealing important information such as user ID and password directly from the wireless system.

In dictionary attack, invaders make use of common usernames and passwords to try to get entry into systems. Common passwords or combinations of characters are encrypted into a dictionary. These encrypted words are then used to compare with those in the system under attack until a match is found. Although this may take weeks or months to be successful, the vulnerability is there for it to become a brute force attack, in which case spam e-mails may be generated while the mail server is opened for such attack.

A fault in the program or application that leads to buffer overflow may create an opportunity for a hacker to overwrite the original code. This kind of buffer overflow attack can cause files to be altered, data to be lost, or even the server to be disabled entirely.

Although measures such as frequently updating security software and applying security patches for operating systems, using antivirus software to block out viruses and worms, firewalls to keep out of the untrusted sites, have more security features for the Web browser, and so on, just to name a few, are in place, but they are not sufficient and safe enough to protect BI, the knowledge capital of an organization, against these security vulnerabilities.

Knowing the fact that BI is too precious to be tampered with by unauthorized use, and too invaluable to be lost or destroyed through security

Electronic Customer Relationship Management (E-CRM) and Customer Loyalty: The Mediating Role of Customer Satisfaction in the Banking Industry
Pushpender Kumarand Anupreet Kaur Mokha (2022). *International Journal of E-Business Research (pp. 1-22).*
www.irma-international.org/article/electronic-customer-relationship-management-e-crm-and-customer-loyalty/293292