

Chapter 7.16

Secure Knowledge Discovery in Databases

Rick L. Wilson

Oklahoma State University, USA

Peter A. Rosen

University of Evansville, USA

Mohammad Saad Al-Ahmadi

Oklahoma State University, USA

INTRODUCTION AND BACKGROUND

Knowledge management (KM) systems are quite diverse, but all provide increased access to organizational knowledge, which helps the enterprise to be more connected, agile, and effective. The dilemma faced when using a KM system is to balance the goal of being knowledge-enabled while being knowledge-secure (Cohen, 2003; Lee & Rosenbaum, 2003).

A recent survey of IT security professions found that over 50% of respondents indicated an increase in the security budgets of their organizations since September 11, 2001, and projected

that 2004 IT security budgets would be larger than ever (Briney & Prince, 2003).

The need for increased security is driven by both monetary concerns and legal/regulatory requirements. The goal of any security architecture, and specifically for KM systems, is to reduce the potential loss caused by intrusion, system misuse, privilege abuse, tampering, and so forth. Protection must be provided against external threats and from internal abuse and must include components that address the requirements for preserving the confidentiality of data where appropriate.

A 2002 Jupiter Research Consumer Survey estimates that as much as \$24.5 billion in online sales will be lost by 2006 due to consumers' lack of

confidence in the privacy of online transactions (E-Compliance Advisor, 2002). While lack of trust is an opportunity cost, security breaches can cause real losses. One study found firms with publicly announced security breaches lose an average of 2% of market capitalization within two days of attack, for an average of \$1.65 billion dollars per breach (Cavusoglu, Mishra, & Raghunathan, 2002). On the regulatory side, legislation like the Health Insurance Portability & Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) have forced companies in health care and financial services fields to improve their security measures (Briney & Prince, 2003; Ingrian Net-

works, 2004). Table 1 summarizes some common security threats.

While most of the major news stories about security breaches involve hackers who steal or access confidential information, infect systems with viruses, and cause trouble with worms or spam, an equally important threat comes from inside organizations. A report from Ingrian Networks (2004) indicated that 50% of security breaches are perpetrated by internal staff (see Lee & Rosenbaum, 2004). Internal threats represent a bigger risk than those from outsiders due to the difficulty in quantifying and counteracting the attacks. But while the risk of insider intrusions

Table 1. Security threats

| Information Source | Ingrian, 2004 | Briney, 2000 | Boren, 2003 |
|--------------------------------|---|---|---|
| General | Poor security policies, human error, dishonesty, abuse of privileges, introduction of unauthorized software | Viruses, malicious code, executables, electronic theft, disclosure of proprietary data, use of resources for illegal / illicit activities | Storage threats: theft of servers, desktops, hard drives, tape backups, information, malicious software installed on server |
| Identification / Authorization | Internal / external attackers posing as valid users / customers | | |
| Reliability of Service | Natural disasters, equipment failures, denial of service | Denial of service, buffer overflows | |
| Privacy | Eavesdropping, unauthorized monitoring of sensitive data | | |
| Integrity / Accuracy | Modification or damaging of information | | |
| Access Control | Password cracking, backdoors, security holes | Protocol weakness, insecure passwords, attacks on bugs in servers | Authentication credentials stolen / not properly managed, users given access to unnecessary information |

9 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/secure-knowledge-discovery-databases/25325

Related Content

The Link Between Knowledge Sharing and Organizational Performance: Empirical Evidence From the Czech Republic

Zuzana Crhová and Jana Matošková (2019). *International Journal of Knowledge Management* (pp. 1-23). www.irma-international.org/article/the-link-between-knowledge-sharing-and-organizational-performance/234376

Citizen Science and Its Role in Sustainable Development: Status, Trends, Issues, and Opportunities

Hai-Ying Liu and Mike Kobernus (2017). *Analyzing the Role of Citizen Science in Modern Research* (pp. 147-167). www.irma-international.org/chapter/citizen-science-and-its-role-in-sustainable-development/170188

Knowledge Sharing Behavior, Mentoring and Motivation as Determinants of Employee Performance in Selected New Generation Banks, Lagos, Nigeria

Oluyinka Titilope Afolayan and Yemisi Tomilola Babalola (2020). *International Journal of Knowledge-Based Organizations* (pp. 57-68). www.irma-international.org/article/knowledge-sharing-behavior-mentoring-and-motivation-as-determinants-of-employee-performance-in-selected-new-generation-banks-lagos-nigeria/248511

Technology Transfer and Innovation Management: The Brazilian TTOs Challenges

Luan Carlos Santos Silva, Silvia Gaia, Carla Schwengber ten Caten and Renata Tilemann Facó (2017). *International Journal of Knowledge Management* (pp. 49-64). www.irma-international.org/article/technology-transfer-and-innovation-management/185764

Indoor Air Quality Monitoring Systems: A Comprehensive Review of Different IAQM Systems

Rasha AbdulWahhab, Karan Jetly Jetly and Shqran Shakir (2021). *International Journal of Knowledge-Based Organizations* (pp. 1-14). www.irma-international.org/article/indoor-air-quality-monitoring-systems/282049