Chapter 8
Preventing Social Engineering and Espionage in Collaborative Knowledge Management Systems (KMSs)

Oluwafemi S. Ogunseye
University of Agriculture, Nigeria

Olusegun Folorunso
University of Agriculture, Nigeria

Jeff Zhang
Ball State University, USA

ABSTRACT

Insider attack and espionage on computer-based information is a major problem for business organizations and governments. Knowledge Management Systems (KMSs) are not exempt from this threat. Prior research presented the Congenial Access Control Model (CAC), a relationship-based access control model, as a better access control method for KMS because it reduces the adverse effect of stringent security measures on the usability of KMSs. However, the CAC model, like other models, e.g., Role Based Access Control (RBAC), Time-Based Access Control (TBAC), and History Based Access Control (HBAC), does not provide adequate protection against privilege abuse by authorized users that can lead to industrial espionage. In this paper, the authors provide an Espionage Prevention Model (EP) that uses Semantic web-based annotations on knowledge assets to store relevant information and compares it to the Friend-Of-A-Friend (FOAF) data of the potential recipient of the resource. It can serve as an additional layer to previous access control models, preferably the Congenial Access Control (CAC) model.

DOI: 10.4018/978-1-4666-2053-7.ch008

INTRODUCTION

If business organizations and governments were cars, knowledge will be the fuel they require to achieve the purpose of their creation, which is movement. As on point as this analogy is, it seems to undermine the importance of knowledge to the different sectors of the world. While we will prevent harping on the issue, we live in a world of competition where there seems to be a conscious agreement (with few exceptions) that in order for knowledge to be valuable for competition, it must be rare, non-imitable and non-substitutable (Uren et al., 2005). Knowledge management concentrates on the processing and storage of documents and the business processes that build on them. These documents provide a rich resource describing what an organization knows (Uren et al., 2005; Sure et al., 2003). They are believed to account for 80-85% of the information stored by many companies. Uren et al. (2005) and Sure et al. (2003) cited contracts, consulting reports, and consumer surveys as examples of documents that can be stored as knowledge resources. Regular web pages can also be formats for knowledge assets.

For systems and organizations to remain relevant and competitive, these knowledge assets must be protected and made scarce to the outside world (Desouza & Vanapalli, 2005). Most research on security of knowledge assets has focused on security against threats from outside sources. These external threats, called intrusions, are handled by access control methods and other techniques. However, the Federal Bureau of Investigation in the US estimated that corporations lose $100 billion, annually, to industrial espionage (Winkler, 1996). This makes clear the fact that insider threats also pose a major problem to business and government systems. This issue of extrusion and insider abuse becomes more delicate when we consider the fact that there is now a continuous rise in alliances between organizations and arguably increasing interests in outsourcing (Desouza & Vanapalli, 2005). Employees, who have all requisite access rights, can send valuable knowledge resource(s) to remote locations or even to partnering (competing) organizations at the detriment of the source organization. In partnering organizations, if two companies A & B are partnering on a project, Company A's employees with access right to company B's Knowledge Systems can abuse that right; stealing valuable knowledge resources from B's organization. As KMSs become more and more semantic web compliant in nature and design, the advantages provided by the design and framework of semantic web can be put to good use in enhancing security for KMSs. Explored in this work are advantages and opportunities, such as this.

KMS FACILITIES OF THE SEMANTIC WEB

Tim Berners-Lee, one of the inventors of the World Wide Web, proposes a more machine-processable web as a development route for the current web. His work on the "semantic web" as an extension of the current web is under progressive research. For the semantic web to work, machines have to be able to not only read web-based information, but also understand it. The term "machines" as used in this statement refers to intelligent agents and software that work on the web. Therefore, these machines should be able to process web-based content including text documents, media, and graphics. This can only be possible through the concept of "intelligent" documents as imagined by the Delphi Group (1994). Intelligent documents are documents that have some degree "self-awareness", meaning that they know who created them, what they might contain, and other information that will enable a machine know what to do with them. This was traditionally accomplished through the use of metadata, but has been replaced with semantic annotations based on domain ontologies (Berners-Lee et al., 2001). The advantages of such annotations are quicker search and retrieval of documents, the automation of several web-based activities, etc. (Gardenfors, 2004; Frienland et