Strategic Importance of Security Standards

Alan D. Smith
Robert Morris University, USA

INTRODUCTION

E-Security and E-Privacy Issues

Even before September 11, 2001, security and privacy was a concern to nearly 80% of the current and potential Internet users around the globe, according to survey released by the Information Technology Association of America (ITAA) (Poulsen, 2000). The survey, commissioned by the American Express Company, randomly polled 11,410 people in 10 countries, and found that nearly half of the respondents enjoyed some form of Internet access. As might be expected, most of the world's Internet users utilize Internet for e-mail, browsing, and entertainment. However, fewer than 28% do some shopping online, and 24% use the Internet for banking and financial transactions. But when Internet users and nonusers of many countries were asked if they agree with the statement, "I am or would be concerned about security and privacy issues when purchasing or making financial transactions online," 79% agreed. Prior to the tragedy of September 11, 2001, U.S. citizens also expressed legitimate concerns toward the issues of privacy and security, with an 85% showing. The poll released by the Information Technology Association of America also illustrated that approximately 80% have doubts about the U.S. government's ability to maintain computer security and privacy. Hence, protecting operating systems is a major strategic concern if the success of e-government as a whole is to reach its potential. Although most of these issues are typically not discussed in relationship with e-government, the need for trusted computing systems within e-business and computing systems can be made as an effective argument that all these issues affect e-government systems as well. Secure computing systems issues in terms of e-government are just as important.

The scope of this article is to present a description of one the most generally known security certifications; namely, the trusted computer system evaluation (TCSEC) and its commercial implementation procedure in the commercial product evaluation process and discuss the influence of this evaluation/certification on the incidence of hacker attacks on e-business. As evident by the abundance of marketing literature of different operating systems for e-business that frequently refers to its security strength ranked against popular security certifications, it is very common to rank commercially available operating systems against TCSEC evaluation and/or certification criteria. This article will also explore where the many operating systems stands on this particular evaluation. In essence, given the vulnerabilities exposed after September 11, 2001, strategic security managers should be deeply concerned that the e-business platform they are responsible for contains the highest security standards to prevent any type of potentially harmful hacker attacks. Managers need to have a working knowledge of TCSEC security evaluation/certifications to become better informed when choosing the e-security platform for e-government/e-business.

Essentially, the selection of a particular operating system for e-government/e-business have as much to do with factors ranging from existing skills, existing infrastructure, and economic reasons all the way up to political and strategic reasons. In dealing strategically with modern e-business environments, one of the most important factors that management must consider when choosing an operating system for their e-business platform is the security strength to resist computer hacker attacks on the operating system. If, for example, during different hacker attacks, one of the major aspects of these attacks is a certain operating system, as opposed to other systems, then this is a clear message to management to build in proper safeguards in the proposed operating system (Smith & Rupp, 2002a, 2002b). Certainly some of the reasons for frequent hacker attacks may probabilistic in terms and not random events, since Linux and Windows operating systems are more frequently used for e-commerce than other systems. So, it is not surprising that there are practically few reports of successful hacker attacks against operating systems that run e-business platforms (Smith, 2005; Smith & Lias, 2005; Smith & Offodile, 2002).

Strategic Imperative for Proper IT Management Practices

Renewed Focus on Security in the E-government Environment

According to Dunn (2001), computer crime incidents more than doubled in a single year, creating a virtual crime wave

across computer systems all over the world. For example, more than 21,000 incidents, up from nearly 10,000 in 1999, were reported in 2000 to Carnegie Mellon University's Software Engineering Institute—which tracks online criminal activity in the United States and provides assistance and advise to victims (CERT/CC statistics 1988-2001, 2001) (This is 5 years old, get the most recent data from the same site.). For example, in the first quarter, record numbers of more than 7000 incidents of cyber crime were posted. As of total incidents reported (1988-Q3 through 2001) has climbed to a record high of 82,465 (CERT/CC statistics 1988-2001, 2001) (Rewrite). The Internet Fraud Complaint Center (IFCC)–which was initially established by the FBI and the National White Collar Crime Center in May 2000, reported increasing amounts of Internet fraud as well (The Internet Fraud Complaint Center (IFCC), 2001). IFCC offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends. The Internet Fraud Complaint Center has reported a total of more than 20,000 complaints from its inception until early November 2000 (The Internet Fraud Complaint Center (IFCC), 2001) (Old data). Unfortunately, in addition to fraudulent transactions, cyber crime ranges from hacking to stealing credit card numbers and planting viruses (Dunn, 2001). The apparent need for strategic management information systems and its proper management to combat these recent and significant increases in cyber crime should be of high priority in the minds of e-government administrators.

Considering that humans cannot be in more than one place at a time, the need for software agents and its document security is on the rise. In order to conduct profitable transactions in the increasing number of electronic marketplaces, an individual user needs to keep tack of the ever-changing offer, demand, and price situations in a secure environment. An encouraging new way of fulfilling this strategy is with the use software agents that represent their human principals at the marketplace, having these agents conduct a whole business transaction in a satisfying way.

A software agent is a computer program which functions continuously and autonomously in an environment in which other processes take place, and other agents exist. In today's environment, agents are known as shopbots, but they are most widely used for information retrieval, while negotiations are not supported. If there is a market world existing without a centralized institution and a common goal, agents will be free to act fraudulently, or cheat in negotiation. In order to reduce the risks related to financial loss in the marketplace due to a fraudulent agent, a mechanism is needed to obtain earlier information concerning the agents' previous transactions- his reputation. The reputation of the agent can be described as good or bad based on the amount of document sharing and former transaction partners apply the rating. A good reputation means that the agent has kept commitments, and an agent having a bad reputation is expected to behave non-cooperatively, or not keep commitments.

The main aspects of a sound security framework, if open to all software agents would be: Authentication, privacy, and non-cooperation. In the occurrence of the authentication issue, the human owner of the agent may choose to mask their identity. In addition, the same person can utilize several different pseudonyms, which in turn may lead to the phantom bidder. Access to change pseudonyms frequently should be unavailable; thus allowing future partners a chance to gain reputation information. The privacy issue is the second area of concern in insecure networks like the Internet, even though confidential communications are subject to prior authentication. Lastly, software agents involved in the marketplace are free to behave in a non-cooperative way.

In order to limit the ability of agents to act irresponsibly, a prototype system called Avalanche was developed, implementing a private key that will digitally encrypt agent messages (Bagner, Evansburg, Watson, & Welch, 2003; Chen, Chen, Lin, 2003; Kang & Han, 2003). The developers believe that this will knock down the barriers that exist for new Internet-based business cooperation. With the help of Avalanche, the development of fast, flexible, and adaptive markets will extend beyond static catalog Web sites and closed auction communities, where transactions amongst unknown agents can create new market opportunities.

In order to take advantage of these new market opportunities, there are numerous research efforts suggesting the need for effective management practices for IT infrastructure and its successful applications. In particular, Ross, Beath, and Goodhue (1996) researched the objectives for successful strategic IT management practice and found the following practices: (1) Bottom aligning IT products and services with the firm's strategic objectives, (2) Delivering solutions faster, and (3) Providing high-quality, cost-effective measures. Ross, Beath, and Goodhue (1996) also found that the process of segregating support costs for non-standard technologies promoted IT-business unit communication that aided in the identification of outdated standards and established priorities for new standards (p. 34). They discovered that shared risk and responsibility are built on this shared communication and mutual respect through the interaction of people and associated IT assets.

In addition, Kossek and Ozeki (1998), make the insightful observation that "The need to develop a global perspective on human resource management has been part of the managerial landscape for well over a decade, but there is no consensus about what tools to use" (p. 2). Kossek