By Bhavani Thuraisingham

DIRECTIONS FOR SECURITY AND PRIVACY FOR SEMANTIC E-BUSINESS APPLICATIONS

Developing secure semantic e-business applications requires focusing first on securing the Semantic Web, knowledge management, and e-business processes.

The Semantic Web is essentially about machine understandable Web pages [3]. One of the main reasons for the rapid development of the Semantic Web is to host e-business applications, which utilize not only the Web, but knowledge management technologies such as ontologies and intelligent information integration [9]. While there has been progress on building valuable applications for the Semantic Web, e-business, and knowledge management, little attention has been paid to security. Here, I discuss some directions to incorporate security and privacy for Semantic-E-business applications.

To secure the Semantic Web, we must protect all its layers, including XML, RDF, ontologies, and information integration. In the case of XML, the security challenges include the granularity of classification as well as secure publication of XML documents. That is, should one classify the entire XML document or only portions of it? Role-based access control for XML documents has also been investigated [4]. Indeed, there has been research on third-party publication of XML documents [5]. Some

WHILE there has been progress on building valuable applications for the Semantic Web, e-business, and knowledge management, little attention has been paid to security.

work on designing security architectures for the RDF model has been explored in [6].

We must ensure the heterogeneous information sources are integrated securely [11]. That is, can we use the ideas presented in secure federated data management for integrating the various information sources? How can the various security policies be integrated? How can we enforce trust management policies across the different sites? How can ontologies be used to specify security policies? There are obviously many challenges to securing these vital processes; a research program focusing on Semantic Web security is greatly needed.

Secure e-business. Security measures for e-business applications have been reported in [7]. The challenges include identifying and authenticating the consumers as well as businesses and tracing all transactions and purchases. One proposed solution is for consumers and businesses to have some credentials when they execute transactions. These credentials, which may be some random numbers, could vary with each transaction. This way the malicious process that masquerades as the business may not have the correct credentials. Moreover, there will be a problem if the credentials are stolen. Various encryption techniques are being proposed for secure e-business processes together with credentials.

Secure supply chain management is another key aspect of secure e-business [2]. The idea is for organizations to provide parts to other corporations for, say, manufacturing or other purposes. Suppose a hospital decides to order surgical equipment from a corporation, there must be some negotiations and agreements between the hospital and the corporation. Corporation X may request some of its parts from Corporation Y and may not want to divulge the fact it is manufacturing the parts for Hospital A. A combination of access control rules and encryption techniques have been proposed as solutions for protecting sensitive information for supply chain management.

Secure knowledge management involves incorporating security into the knowledge management cycle. That is, a corporation must protect its intellectual property and trade secrets using secure knowledge management strategies, processes, and metrics. Knowledge management is a cyclic process [8], therefore security measures must be incorporated into all aspects of the process. For example, when knowledge is created, that knowledge must be protected. When knowledge is represented, the security policies must be represented as well. Knowledge manipulation and dissemination involves enforcing the security policies. And the actions taken must consider security.

Secure knowledge management strategies involve creating plans to share and enhance the knowledge in accordance with the security policies. We must also investigate the security impact of metrics, that is, the means for measuring the knowledge (for example, the number of patents obtained by a corporation). Finally, technologies for knowledge management such as the Semantic Web must be secure.

Secure integration of the Semantic Web, knowledge management, and e-business processes poses many challenges. Suppose two corporations want to carry out a transaction. They may both log into their Semantic Webs and use a variety of information interoperability tools to exchange data and information. Various access control and usage control policies will be applied to ensure the users can carry out the operations and access the data. The e-business processes specify the operations to be carried out to complete the transactions. The organizations that execute the e-business processes must execute permissions. Finally, secure knowledge management tools are utilized to determine what information and resources are needed for the transaction and whether the information and resources can be accessed by the organizations involved.

Essentially, security must be incorporated into all aspects of the Semantic E-business process. Trust management and negotiations play an important role. How much trust do the organizations place in one another? How can one trust the quality of the data and information sources? We need flexible policies that ensure security and timely information processing depending on the applications and the particular scenarios. We need research and development efforts on developing a security framework for semantic e-business applications.

Privacy Aspects

Data mining is also being applied for e-business applications, such as targeted marketing, customer information management, and business intelligence. While data mining is useful for many applications, it is also a serious threat to security and privacy [10]. Data mining users now have access to the various tools, and as a

result can infer sensitive and private information. Inference control techniques as well as privacy preserving data mining techniques are being investigated [1].

The Semantic Web has inference capabilities built into it. This would exacerbate the inference and privacy problems. Therefore, we must examine inference control and privacy preserving data mining techniques and determine their applicability for the Semantic Web. We must also examine security and privacy at the onset and not as an afterthought. Furthermore, we must explore the implications of security and privacy for Semantic E-business applications that result from data mining and information extraction.

Conclusion

This article provides some initial directions for security and privacy for Semantic E-business applications. We discussed security for the Semantic Web, e-business, knowledge management, and integration, as well as semantic Web mining and the implications for security and privacy.

Research on Semantic E-business is just beginning. There is still a lot to do before we can develop secure semantic e-business applications. We need a focused research program that addresses security for the Semantic Web and its many layers. Privacy implications due to Semantic Web mining also need attention as does the need to develop a security framework for Semantic E-business applications. C

References

1. Agrawal, R, and Srikant, R. Privacy-preserving data mining. In *Proceedings of the ACM SIGMOD Conference,* (Dallas, TX, May 2000).
2. Atallah, M. et al. Secure supply-chain protocols. In *Proceedings of the International Conference on Electronic Commerce*, 2003.
3. Berners-Lee, T. et al. Hendler, J. and Lassila, O. The Semantic Web. *Scientific American*, 284, 5. (May 2001) 34–43.
4. Bertino, E. et al. Access control for XML documents. *Data and Knowledge Engineering,* (2002).
5. Bertino, E. et al. Secure third-party publication of XML documents. *IEEE Trans. on Knowledge and Data Eng.* (Oct. 2004).
6. Carminati, B. et al. Specifying security policies in RDF. In *Proceedings of the DEXA Workshop,* 2004.
7. Hassler, V. *Security Fundamentals for E-Commerce.* Artech House, UK, 2000.
8. Morey, D. et al., Eds. *Knowledge Management.* MIT Press, 2001.
9. Singh, R. et al. Semantic e-business. *Intern. J. on Semantic Web and Information Systems* (2004).
10. Thuraisingham, B. Data mining, national security, privacy and civil liberties. *SIGKDD Explorations,* 2002.
11. Thuraisingham, B. Security standards for the Semantic Web. *Computer Standards and Interface J.* (Mar. 2005).

Bhavani Thuraisingham (bhavani.thuraisingham@utdallas. edu) is a professor of computer science and director of the Cyber Security Research Center at the University of Texas at Dallas.