Formal modeling and analysis of XML firewall for service-oriented systems

Haiping Xu*, Mihir Ayachit and Abhinay Reddyreddy
Computer and Information Science Department,
University of Massachusetts Dartmouth, North Dartmouth, MA 02747, USA
E-mail: {hxu, g_mayachit, g_areddyreddy}@umassd.edu
*Corresponding author

Abstract: As more businesses deploy web services over the Internet, the issue of how to secure them from intruders and possible threats becomes more important. Firewalls have been designed as a major component to protect a network or a server from being attacked. However, since conventional firewalls emphasize on packet filtering at the transport and session layer, rather than verifying user permissions and examining packet contents at the application layer, they are not suitable for protecting service providers from unauthorized web service invocations. In this paper, we propose a formal XML firewall security model using role-based access control (RBAC) mechanisms. Our proposed formal model supports user authentication and role-based user authorization according to policy rules stored in a policy database that can be updated dynamically. The formal model is designed compositionally using colored Petri nets (CPN), which can serve as a high-level design for XML firewall implementation. The major components of our compositional XML firewall security model are the application model and the XML firewall model. We analyze the application model and the XML firewall model separately using an existing Petri net tool, called CPN Tools, and demonstrate how key properties of our formal models can be verified, and how a design error can be detected and corrected at an early design stage.

Keywords: XML firewall, web services, service-oriented systems, role-based access control (RBAC), colored Petri net (CPN), formal verification.

Reference to this paper should be made as follows: Xu, H., Ayachit, M., and Reddyreddy, A. (2008) 'Formal modeling and analysis of XML firewall for service-oriented systems', *Int. J. Security and Networks*, Vol. 3, No. 3, pp. 1-13.

Biographical notes: Haiping Xu received the Ph.D. degree in computer science from the University of Illinois at Chicago in 2003. He is an assistant professor in the Computer and Information Science Department at the University of Massachusetts Dartmouth, where he is a co-director of the Concurrent Software Systems Laboratory. His research interests include distributed software engineering, formal methods, Internet security, multi-agent systems, and service-oriented systems. He is a member of the ACM and the IEEE Computer Society. Mihir Ayachit received the M.S. degree in computer science from the University of Massachusetts Dartmouth in 2006. He is currently a software engineer in Parametric Technology Corporation. His research interests include web services security, formal methods, and model-based software development. Abhinay Reddyreddy is currently a graduate student in the Computer and Information Science Department at the University of Massachusetts Dartmouth. His research interests include web services security and formal methods for specification and analysis of concurrent and distributed software, especially the application of Petri net-based models.