Introduction

Web services security has been a challenging issue in recent years because current security mechanisms, such as conventional firewalls, are not sufficient for protecting service-oriented systems from XML-based attacks. In order to provide effective security mechanisms for service-oriented systems, XML firewalls were recently introduced as an extension to conventional firewalls for web services security. In this project, we introduce a state-based XML firewall architecture that supports role-based access control and real-time detection of XML-based attacks. We develop a detailed design of the state-based XML firewall by defining state-based information, user information, and various access control policies and detection rules. To illustrate the effectiveness of our approach, we develop a prototype state-based XML firewall, and demonstrate how XML-based attacks can be efficiently detected.

State-Based XML Firewall

- Comes from a Petri net based XML firewall formal model we proposed previously.
- Grants only those users who are properly authenticated and authorized for access of web services.
- Adopts dynamic role-based access control (RBAC) for user authorization.
- Is supported by policy rules based on user information and state information.
- Role-based access control policy rules for user authentication and authorization.
- Detection rules for identifying XML-based security threats.
- Can examine the contents of incoming XML-based messages (SOAP messages).

Design of Policy Rules

Role-Based Access Control Policies

- Specify the roles that a user may adopt and the permissions associated with each role.
- Examples of role-based access control policy rules.

Real-Time Detection of XML-Based Attacks

- SOAP filter is responsible for real-time detection of XML-based attacks.
- Example of suspicious XDoS attack detection rules.

Conclusions

We introduced a state-based XML firewall, which can be used to protect a service provider from various XML-based attacks. We also developed a detailed design and implemented a prototype state-based XML firewall. For more information, please refer to web: http://www.cis.umassd.edu/~hxu/Projects/XMLFirewall

Acknowledgements

This work is supported by the Chancellor’s Research Fund/Healey Endowment Grants, and the Research Seed Initiative Fund (RSIF), COE, UMass Dartmouth.