Development of a Web Service Probing Tool

Background

The SOA Security Lab is a cloud platform that enables the testing, monitoring and analysis of Web Services regarding different security configurations, security concepts and infrastructure components. A SOA Security Lab user can create a graphical system design model which will be made executable by the Lab. To enhance the security experience for a user, it shall be possible to attack the executed system components (Web Services) interactively using known Web Service attacks. In addition, this tool should be usable to find or create new attacks based on the knowledge about the system components.

Description

In a first step for the development of the Web Service Probing Tool, a gateway solution is required to capture, store and forward Web Service messages. Based on this gateway, a Plug-in mechanism has to be created to provide the different Web Service attacks to the system. For the usability of the tool, a basic web based user interface for the different attacks is required, as well. As a proof, that the system is working correctly, some Web Service attacks, like SOAPAction Spoofing and XML-Signature-Wrapping, have to be implemented. In addition, countermeasures for the implemented attacks can be proposed to the user, to prevent these attacks in the future.

References

- Website of the SOA Security Lab: www.soa-security-lab.de
- „SOA Security Kompendium“, Bundesamt für Sicherheit in der Informationstechnik, 2010

Contact

Internet Technologies and Systems

- Prof. Dr. Christoph Meinel
- Robert Warschofsky, M.Sc.