Karlsruher Institut für Technologie

Certifiable Trustworthy IT Systems
Am Fasanengarten 5
76131 Karlsruhe
Web: http://zvi.ipd.kit.edu

Implementation of HTTPS with XML-RPC

Hiwi assignment

Supervisors: Prachi Kumari, Prof. Dr. Alexander Pretschner
Email: {prachi.kumari, alexander.pretschner} @ kit.edu
Phone: +49 721 608 5082
Starting date: immediately
Prerequisites: LAMP – Windows/Linux, Apache HTTP Server, MySQL and PHP; Practical knowledge of computer networking and cryptography

Introduction

Usage control requirements specify restrictions and compulsory actions that relate to the future handling of data. These requirements can/must be enforced at different levels of abstraction within a system (e.g. operating system, windowing system, java byte code, service level, etc.) and across systems also. This is because data has different representations at different levels of abstractions in different systems. Similarly, actions, like “copy” or “delete” etc. also have different semantics at all these levels. In order to control the usage of a specific data, we need to monitor and track actions performed over all of the representations.

This assignment is about data security at the network layer. XML-RPC is a remote procedure call (RPC) protocol which uses XML to encode its calls and HTTP as a transport mechanism. However, HTTP communication is vulnerable to malicious attacks like man-in-the-middle. As a countermeasure, SSL/TLS protocols are used at the underneath layers to provide encrypted and secure communication at the application layer. A major challenge is the management of encryption keys.

Work package

The goal of this assignment is to replace existing HTTP communications with HTTPS implementations in an existing web application. There are two HTTP connections that need to be secured, one of them using XML-RPC messages. The major problem to be addressed in this case is key management while implementing certificates.

Submission of the following is mandatory at the end of the assignment:

1. Raw code
2. Code in executable format
3. Virtual machine(s) for demo of the work
4. Documentation explaining the set up and usage of the code and the virtual machine(s)

Work Plan

1. Familiarize yourself with the existing system.
2. Complete the workpackage.
3. Submit your work as explained above.

References and further readings

[1] Overview of XML-RPC at Wikipedia, http://en.wikipedia.org/wiki/XML-RPC [Accessed: October 13, 2010]
[2] XML-RPC Home Page, http://www.xmlrpc.com/ [Accessed: October 13, 2010]
[3] RFC 2818 http://tools.ietf.org/html/rfc2818 [Accessed: October 13, 2010]