Applying End-to-End Security Across an Apache Tomcat Web Environment

Event

ApacheCon Core Europe
Submission Type Tutorial
Category Developer
Status New

Abstract

This tutorial covers how to apply an end-to-end application security architecture using Apache products like Tomcat, ApacheDS and Fortress. It will be divided into four 30 minute segments: 1. Install security infrastructure: ApacheDS and Fortress. 2. Deploy a simple Java Web app into Apache Tomcat. Get authentication and coarse-grained authorization enabled to control page access. 3. Add fine-grained authorization to Web application controls (buttons, list boxes, ...) and database functions (create, read, update, delete). 4. Generate keys and certs, enable TLS to HTTP, LDAP and JDBC connections. The student will leave with understanding to apply proper security techniques to Web apps. A number of relevant standards including Java EE Security, Role-Based Access Controls (ANSI INCITS 359), Transport Level Security (TLS), and X.509 are followed. The sample code uses Java.

Audience

Java developers, security administrators and mangers who need hands-on knowledge with application security techniques within HTTP runtime environments. This tutorial uses Java but the same techniques apply to other platforms.

Experience Level

Intermediate

Benefits to the Ecosystem

Attendees benefit by understanding security requirements. They will be provided a tutorial to satisfy the requirements using available open source tools. But the biggest benefit will be to the users. Techniques learned here will safeguard their electronic assets.

Technical Requirements

Student/Machine/Network Prerequisites: 1. Java programming knowledge and familiarity with Apache Tomcat 2. Debian or Centos Linux Machine 3. 2GB RAM 4. Connection to Internet (for dependencies)