Introduction to Apache Shiro

What is Apache Shiro?

Apache Shiro is a powerful and flexible open-source security framework that cleanly handles authentication, authorization, enterprise session management and cryptography.

Apache Shiro's first and foremost goal is to be easy to use and understand. Security can be very complex at times, even painful, but it doesn't have to be. A framework should mask complexities where possible and expose a clean and intuitive API that simplifies the developer's effort to make their application(s) secure.

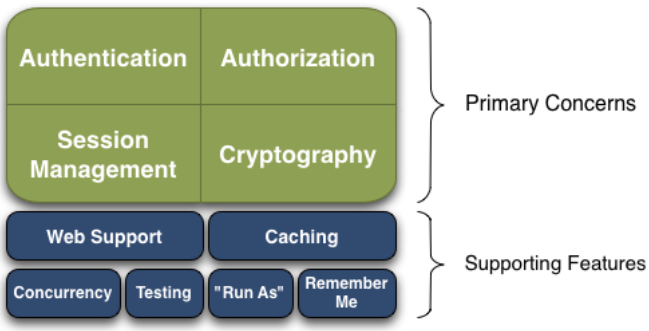
Here are some things that you can do with Apache Shiro:

- Authenticate a user to verify their identity
- Perform access control for a user, such as:
  - Determine if a user is assigned a certain security role or not
  - Determine if a user is permitted to do something or not
- Use a Session API in any environment, even without web or EJB containers.
- React to events during authentication, access control, or during a session's lifetime.
- Aggregate 1 or more data sources of user security data and present this all as a single composite user 'view'.
- Enable Single Sign On (SSO) functionality
- Enable 'Remember Me' services for user association without login
  ...
  and much more - all integrated into a cohesive easy-to-use API.

Shiro attempts to achieve these goals for all application environments - from the simplest command line application to the largest enterprise applications, without forcing dependencies on other 3rd party frameworks, containers, or application servers. Of course the project aims to integrate into these environments wherever possible, but it could be used out-of-the-box in any environment.

Apache Shiro Features

Apache Shiro is a comprehensive application security framework with many features. The following diagram shows where Shiro focuses its energy, and this reference manual will be organized similarly:



Shiro targets what the Shiro development team calls "the four cornerstones of application security" - Authentication, Authorization, Session Management, and Cryptography:

- **Authentication:** Sometimes referred to as 'login', this is the act of proving a user is who they say they are.
- **Authorization:** The process of access control, i.e. determining 'who' has access to 'what'.
- **Session Management:** Managing user-specific sessions, even in non-web or EJB applications.
- **Cryptography:** Keeping data secure using cryptographic algorithms while still being easy to use.

There are also additional features to support and reinforce these concerns in different application environments, especially:

- Web Support: Shiro's web support APIs help easily secure web applications.

- Caching: Caching is a first-tier citizen in Apache Shiro's API to ensure that security operations remain fast and efficient.
- Concurrency: Apache Shiro supports multi-threaded applications with its concurrency features.
- Testing: Test support exists to help you write unit and integration tests and ensure your code will be secured as expected.
- "Run As": A feature that allows users to assume the identity of another user (if they are allowed), sometimes useful in administrative scenarios.
- "Remember Me": Remember users' identities across sessions so they only need to log in when mandatory.