Spring Security

Beginner to Guru

Remember Me Overview

Remember Me Overview

- Remember Me is a technique of allowing a web application to ‘Remember’ the login details of a user
- Allows user to stay signed into web application, without having to login again
    - Logins in Java are typically tracked with a session id, which is short lived
- Remember Me is implemented by storing user details in a cookie
    - Application uses cookie details to authenticate user upon their return
    - Cookie can be set to expire after X period of time

Remember Me Overview

- Remember Me is typically done by user opt-in
  - User should not use Remember Me on public computers
  - Should not be done automatically

Remember Me Problems

- Data in Remember Me is used to authenticate
- If compromised, the Remember Me cookie could be used to impersonate the user
  - Effectively a username and password rolled into a cookie
- Best practice is to never send Remember Me cookies over HTTP
  - Always use HTTPS to protect cookies from third parties

Remember Me Precautions

- Due to potential compromise of Remember Me Cookies, sensitive functions should be restricted
- Spring Security has methods for ‘isRemembered’ or ‘isAuthenticatedFully’
- Require full authentication for functions such as:
  - Password change
  - Email change
  - Update of personal information - name, address, payment information, etc
  - Making purchases

Spring Security Remember Me

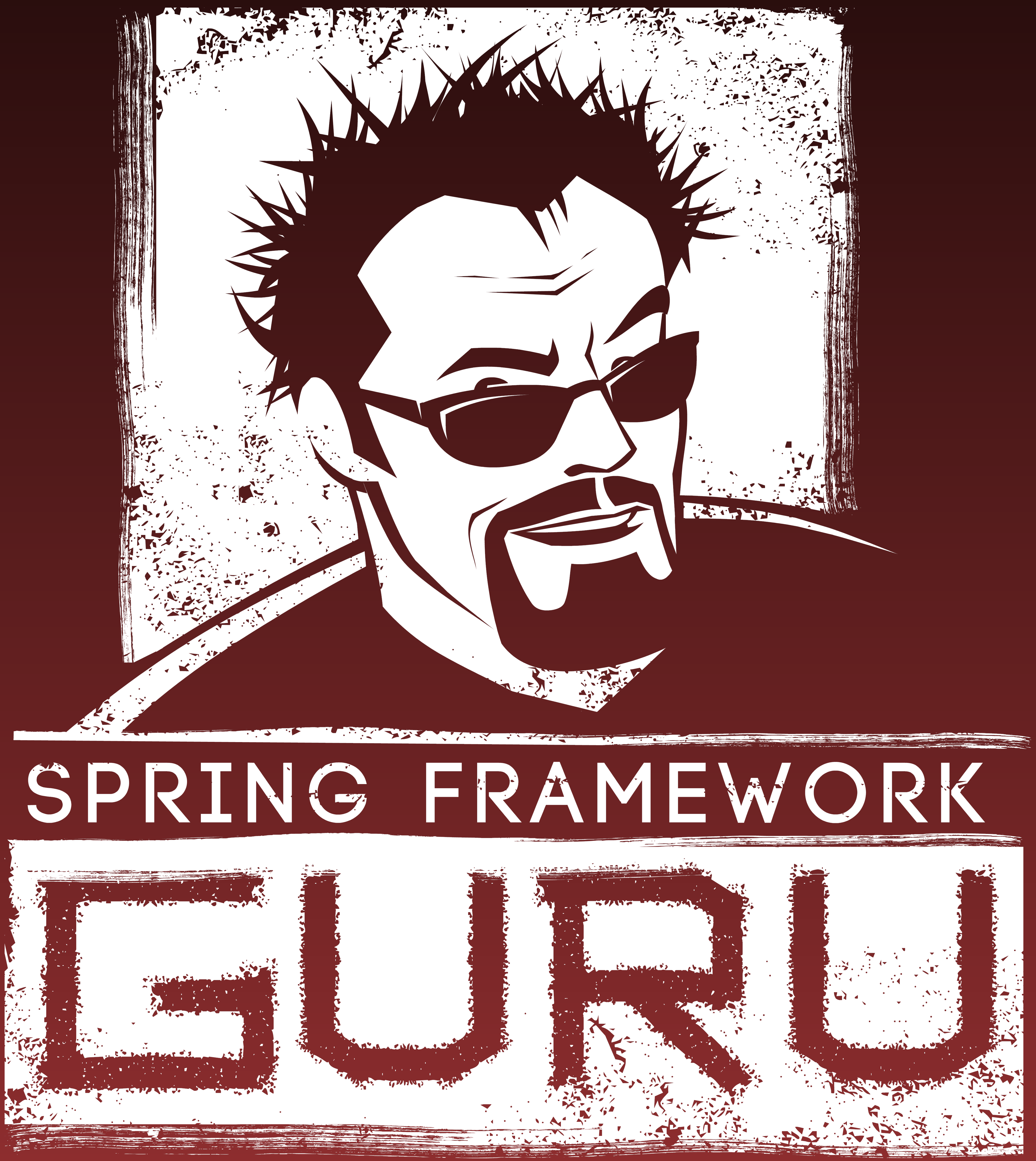
- Spring Security provides two remember me implementations
  - Simple Hash-Based Token
  - Persistent Token
- Both implementations required a UserDetailsService
  - Not all authentication provides have a UserDetailsService
    - For example, LDAP

Simple Hash-Based Token

- The Simple Hash-Based Token is a Base64 string consisting of:
    - `base64(username + ":" + expirationTime + ":" + md5Hex(username + ":" + expirationTime + ":" password + ":" + key))`
- The advantage of having the password in the hash is the user can change their password and invalidate all remember me tokens
- Can support multiple browsers / computers
- Attacker can use cookie until it expires or password is changes

Persistent Token

- Remember Me Cookie contains: username, a series id, and a token (random string)
  - These values are persisted to the database
- On login via Remember Me values are fetched from database
  - If matched, user is authenticated, and new token is created for series id (browser / devices)
  - If username and series match, but token does not, theft is assumed
    - Delete all tokens for user
  - Shortens attack window until real user logs in vs expirationTime
  - From Drupal CMS


SPRING FRAMEWORK
GURU