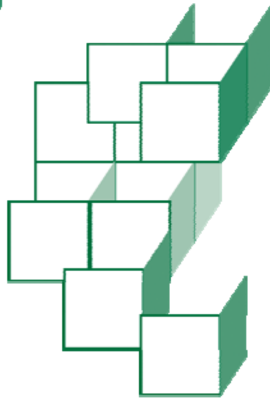
Chapter 3

URL Authorization



OBJECTIVES

After completing "URL Authorization," you will be able to:

- Develop fine-grained authorization policies over your web application's request URLs.
- Use the Spring Security API to discover information about the current user, and to make programmatic authorization decisions.
- Show pieces of user interface conditionally, based on authority.

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

URL Authorization

- **The first and most common sort of authorization policy for web applications requires that the user be in one of a list of roles in order to get a response for a certain request URL.**
- **In Spring Security we do this with the `<intercept-url>` element.**
  - The **pattern** attribute identifies one or more URLs to be protected. This is interpreted by a pluggable pattern-matching algorithm.
  - By default, patterns are **Ant-like**: they can be single URLs or masks using wildcards `*` (any token) and `**` (any path).
  - They are **context-relative**, so should use a leading `/` character.
  - We can further narrow the constraint by specifying an HTTP **method**, such as "GET" or "POST".
  - Then the **access** attribute identifies one or more roles: the user must be playing at least one of these, to avoid the dreaded 403.
  - The **filters** attribute allows one or more filters in the configured filter chain to be dropped out for this URL pattern. In practice this is generally either left out or it's "none" to open all access.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

URL Authorization

- **`<intercept-url>`s are processed in the order of declaration**
  - **First match** sets the rules, and the rest are ignored.
  - This is another difference from servlet-container authentication, where there are more complex rules about what constraints override what others, and the general idea is order doesn't matter and specific patterns should trump general ones.
  - In Spring Security, it's entirely up to you to put things in the proper order, as a general pattern will take precedence over a more specific one that follows – and this is usually not desired.
  - Then, two general-purpose patterns might overlap – consider the following – and it's a design question which one should go first.

```
/admin/**
/**/*.xml
```

- **By default, role names must all begin with "ROLE_".**
  - This is a common pitfall in working with Spring Security, as developers will often assume that any unique string is fine and define roles such as "user", "admin", "member", etc.
  - Then everyone gets a 403, and it can take some digging and trial-and-error to discover the root cause.
- **This can be configured, by a couple of strategies, and we'll consider this further in the following chapter.**

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Who Goes There?

- In **Examples/Login/Step5**, we have a few specific page constraints and a catch-all – see **docroot/WEB-INF/applicationContext.xml**.

```
<http>
  <intercept-url pattern="/login.jsp"
                 filters="none" />
  <intercept-url pattern="/index.jsp"
                 access="ROLE_ANONYMOUS" />
  <intercept-url pattern="/protected.jsp"
                 access="ROLE_ADMIN" />
  <intercept-url pattern="/**"
                 access="ROLE_USER"/>
  ...
```

- We've seen the results of this policy:
  - Any **user** can see the index page and the login page – though by two mechanisms, filter bypassing vs. anonymous authentication.
  - Any **authentic user** (ROLE_USER) can see those plus **home.jsp**.
  - An **administrator** (ROLE_ADMIN) can see everything.
- You can give this a quick try now, if you like:
  - Login as **friend/trustme** and try to visit the protected page ...

Authorization Failure

You are not authorized to view the requested page.

  - Login again as **overlord/fearme** and get through.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

The Healthcare Case Study

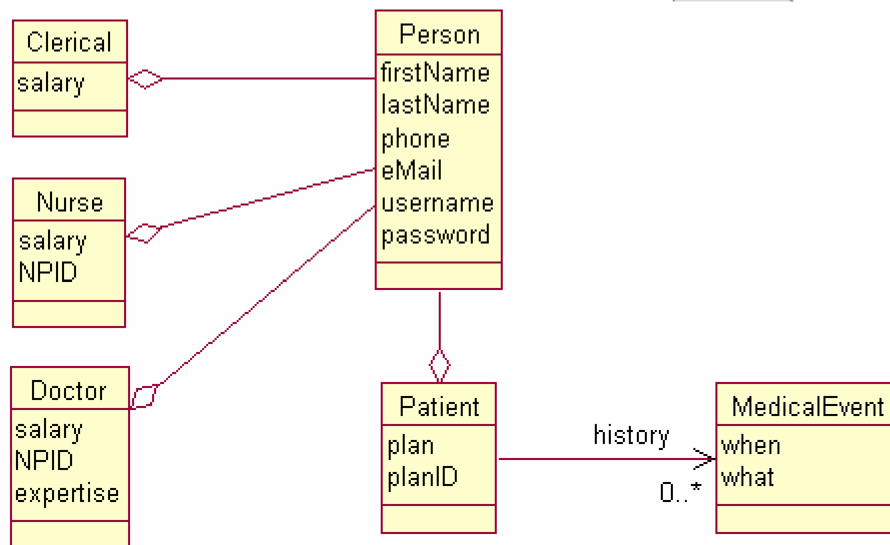
- **We've worked with the Health application a bit already, but as we get into implementing a full authorization policy (which you're about to do in the upcoming lab), it's worth a little time to get more familiar with its functionality.**
- **The Healthcare application implements a handful of functions for a healthcare system.**
- **It has a database of doctors, nurses, patients, and clerical staff – all of whom are potential users of the application as well.**
  - **Java Persistence API** (**JPA**) entities are mapped to this database and form the primary domain model.
- **Main use cases are as follows, and are implemented by servlets and JSPs:**
  - Users can **modify their profiles**, and this includes changing their usernames and passwords.
  - Users can **make appointments** between doctors and patients.
  - Doctors, nurses, and a patient himself or herself can view the patient's **medical history**.
  - Doctors can **prescribe medication**.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Domain Model

- Here is a UML class diagram representing the domain model:



  – Not shown is the **id** field for each entity, which maps to a generated primary key value in the database.

- At the database level, the schema also includes a SQL VIEW that presents each of the **Doctor**, **Nurse**, **Clerical**, and **Patient** types as role names to Spring Security.

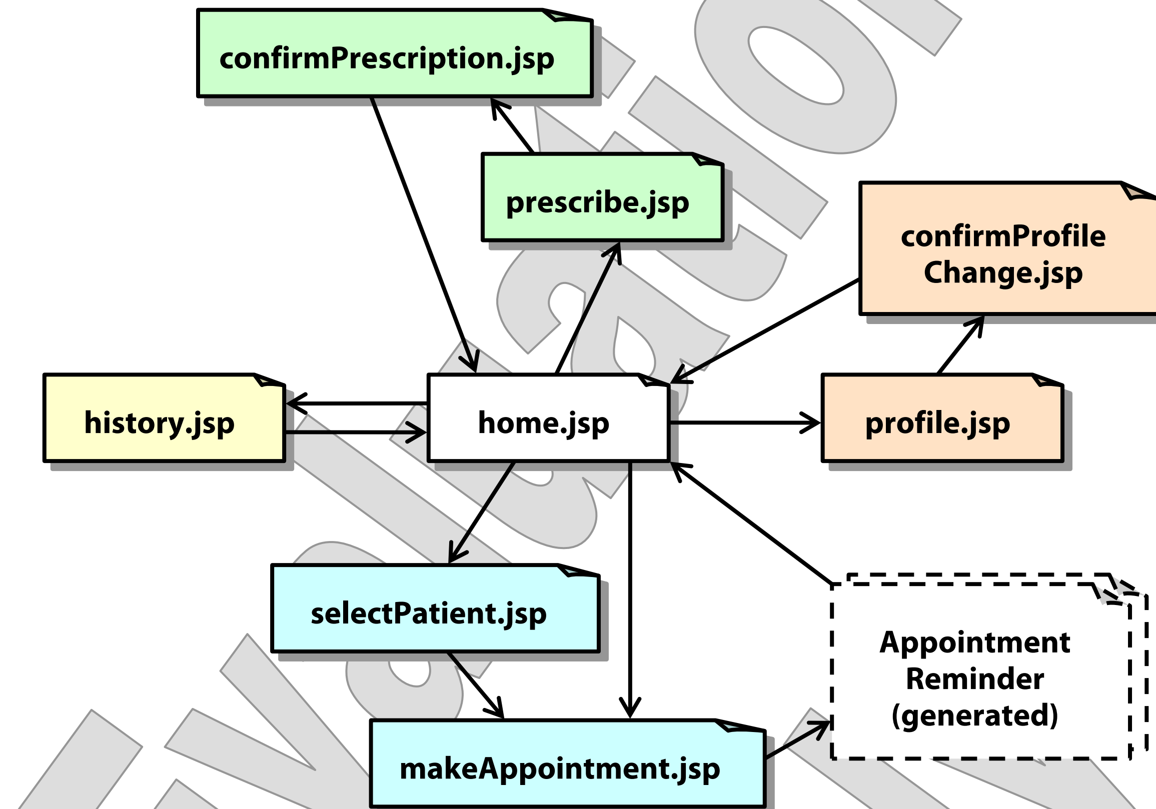
```
ROLE_PATIENT
ROLE_DOCTOR
ROLE_NURSE
ROLE_CLERICAL
```

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Page-Flow Model

- The user can carry out those four use cases, each by clicking a link on the home page and following a short page flow that resolves back to home:



  – Not shown are various servlets and filters that manage information flow between pages.

Evaluation Only

Roles and Privileges

- **Only certain roles are appropriate to some functionality:**
  - Anyone can see and change their own **user profile**.
  - Anyone can **make an appointment**; a patient should only be able to make an appointment for himself or herself.
  - Doctors and nurses should be able to see **medical histories**; and patients should be able to see their own, but not others'.
  - Only doctors should be able to **prescribe medication**.
- **More subtly, the application should behave differently depending on the role(s) assigned to the interactive user.**
  - If the user is a patient, then the **choice of patient** for showing medical history or making an appointment should be implicit; if the user is a doctor, nurse, or clerical worker, he or she should be given a chance to select a patient.
  - This switch is implemented for medical history: a servlet checks the logged-in user and determines whether the **selectPatient.jsp** should be shown before moving on to **showHistory.jsp**.
  - It is not yet implemented for appointments; that will be one goal of an upcoming lab.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Healthcare Users: a Cheat Sheet

- As you work on the upcoming lab, you will need to log in variously as different patients, doctors, nurses, and staff.
- There are about 50 total users in the database, but below are a small set of logins that you can use for your testing:
  - Patients:

```
Lesa_Griffith/globalVILLAGEidiot
beard/password
burgess/CAVEman
```

  - Doctors:

```
dtravis/sadlyECSTATIC
feelgood/mrsmd
church/hEoTpEeRsNpArLings
```

  - Nurses:

```
Nola_Mullins/miffmufferedmoof
Edgar_Frank/OFTENTIMES889 (note: also a patient)
ratched/meanie
```

  - Clerical staff:

```
hebert/invisible^JUMP!SUIT
Larry_Best/if_you_cAn_guess+THIS
                          (note: also a patient)
martinez/CavesOfAltamira
```

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Healthcare URL Authorization

Suggested time: 30 minutes

In this lab you will build a fine-grained authorization policy for the Health application, based on request URLs and the requirements stated earlier. You will write out **`<intercept-url>`**s to express specific constraints and allow doctors, nurses, clerical staff, and patients variously to access those URLs.

Detailed instructions are found at the end of the chapter.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Programmatic Authorization: Servlets

- Everything we've seen so far is **declarative**, and this is a selling point: we state the security requirements for an application, and Spring Security enforces them.
- There is also a **programmatic** approach, which can be mixed and matched with the declarations we've seen already.
- For this purpose, **HttpServletRequest** offers a few methods that are easy to use and well-known to most servlet programmers:

```
public interface HttpServletRequest
{
  public Principal getUserPrincipal ();
  public String getRemoteUser ();
  public boolean isUserInRole (String roleName);
}
```

- Using these methods you can get
  - The principal record itself – which may be of any subtype of **Principal** and offer any amount of information specific to the authentication system, but will always provide paths to username and assigned roles
  - The primary name of the authenticated **user**
  - Whether that user is in a desired **role**
- It is <u>not</u> necessary to refactor existing servlets code to adapt to Spring Security once you've put it in place.
  - Rather, Spring Security adapts to the servlets standard: one filter in the chain wraps the container-built request object in one that will implements these methods to use the Spring Security API.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Programmatic Authorization: Spring Security

- **New applications that don't mind developing some code-level dependencies on Spring Security can use the API directly.**
- **There are several avenues of approach – and now the drumbeat for Chapter 4 and a deeper study of the API is getting pretty loud! – but the simplest of these are as follows.**
- **To get the current user – this is equivalent to getPrincipal or getRemoteUser – use the following incantation:**

```
SecurityContextHolder.getContext ()
  .getAuthentication ().getPrincipal ()
```

  – This gives you an object which you can downcast to the type **Authentication** and then query for username, roles, etc.

  – The security context is **thread-affinite**, so you don't need a servlets-level request object, or anything else.

- **To check for roles/authorities more directly, try this:**

```
AuthorityUtils.userHasAuthority ("ROLE_SOMETHING")
```

  – This returns a boolean and is by far the easiest way to do programmatic security with the API.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

When to Use Programmatic Authorization

- **Declarative security is preferred whenever it can precisely express the authorization policy.**
- **Programmatic security steps in when more fine-grained decisions must be taken:**
  - If credentials are drawn from a larger body of persistent domain objects, the application may well want to **determine who is logged in**, so as to represent information about that user without having to ask twice.
  - **Different behavior** might occur based on user identity or role. For example, we might want to show certain UI content, or go to entirely different pages, based on role.
  - Sometimes an HTTP request will trigger a **complex business process**, only some of which would be carried out if the user were not in a sufficiently powerful role.
  - Different **error handling** might obtain for administrators than for ordinary users.
- **Many applications combine declarative and programmatic techniques:**
  - Declare security constraints that, by themselves, might allow unauthorized access or functionality.
  - Weed out those remaining cases programmatically.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Role-Based Presentation

- **It's rather rude to invite the user to click a button or a link that would request a URL they can't actually request, and then serve them up a 403 error message.**
  - Ideally, such errors should only appear in cases of forceful browsing, where the user explicitly requests a specific URL.
- **Better to guide the user only to choices that he or she is in fact authorized to make.**
- **This means showing certain pieces of a UI conditionally, based on the authenticated user's role assignments.**
- **This can be a little bit of a chore in Java EE.**
  - For one thing, the **isUserInRole** method isn't JSP-friendly: we can't write a JSP expression to test that. (If there were a map of the user's **roles**, we'd be in great shape ... but, no.)
  - Also, in order to solve the problem generally, one must have some enumeration of all the roles supported by the application – again, **isUserInRole** won't volunteer information.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

The Spring Security Tag Library

- **To the rescue comes a small tag library, distributed with Spring Security, that gives JSPs some programmatic security capabilities.**
- **Declare this tag library as follows (we use the prefix sec: but as with all tag libraries the prefix is up to you):**

```
<%@
  taglib prefix="sec"
  uri="http://www.springframework.org/security/tags"
%>
```

- **Use the `<sec:authorize>` tag to wrap content that should be produced only if the user has a certain role or certain roles.**

```
<sec:authorize ifAnyGranted="ROLE_ADMIN" >
  <p>The secret monitoring data is ${mon.data}</p>
</sec:authorize>
```

  - The **ifAnyGranted** attribute lists one or more roles, any of which, if granted, will cause the tag to produce its body content.
  - You can also specify **ifAllGranted** to require multiple roles.

- **You can also show content in case the user is not authorized to a certain function – perhaps some static text in replacement for the dynamic content you would otherwise be showing.**
  - Use the **notGranted** attribute, which will cause content to be shown if none of the listed roles are in force.

- **There is also a tag that gives direct access to properties of the Authentication object representing the current user:**

```
<sec:authentication property="principal.username"/>
```

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

Suggested time: 30 minutes

In this lab you will add role-based presentation to the home page of the Health application, guiding the user only to the functions to which he's authorized, using the Spring Security tag library.

You'll also review some programmatic security already implemented in the medical history feature, and fix one remaining piece of code so that the page flow for staff vs. non-staff users is different when making appointments.

Detailed instructions are found at the end of the chapter.

Evaluation Only

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.

SUMMARY

- **We've done quite a lot with Spring Security at this point – and notice that, except for the most recent lab, we've done no Java coding, just XML configuration and some work in JSPs.**
- **There is more to Spring Security, and with many of the features below we do cross that line and need to start building Java classes that extend or plug into the framework.**
  - Custom authentication providers
  - Adding your own filters to the chain
  - Instance-level authorization
- **Other features can still be done purely with declaration, but require more familiarity with the underlying mechanism of Java classes, and that the developer work at a lower level with plain old `<bean>` definitions of those classes.**
  - Channel security
  - HTTP DIGEST
  - Localization
  - Using JAAS
  - Run-as identities

Page	Doctor	Nurse	Clerical	Patient
Home page, CSS, etc.	X	X	X	X
Medical history	X	X		X
User profile	X	X	X	X
Appointments	X	X	X	X
Prescription	X			

© 2006-2010 Will Provost.
All Rights Reserved by Capstone Courseware, LLC.