CASifying the Big Green

Technical Details

Steve Cochran

JA-SIG Summer Conference

June 26th 2007

Who Am I

Manger, Special Projects
Dartmouth College

- Ongoing Responsibilities:
  - Directory
  - Authentication
  - Email
  - Calendaring
  - Web and File Services
- Recent Projects
  - WebAuth, Paperless Admissions Office, “Smart” System Status Notification, Authenticated Network Access

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

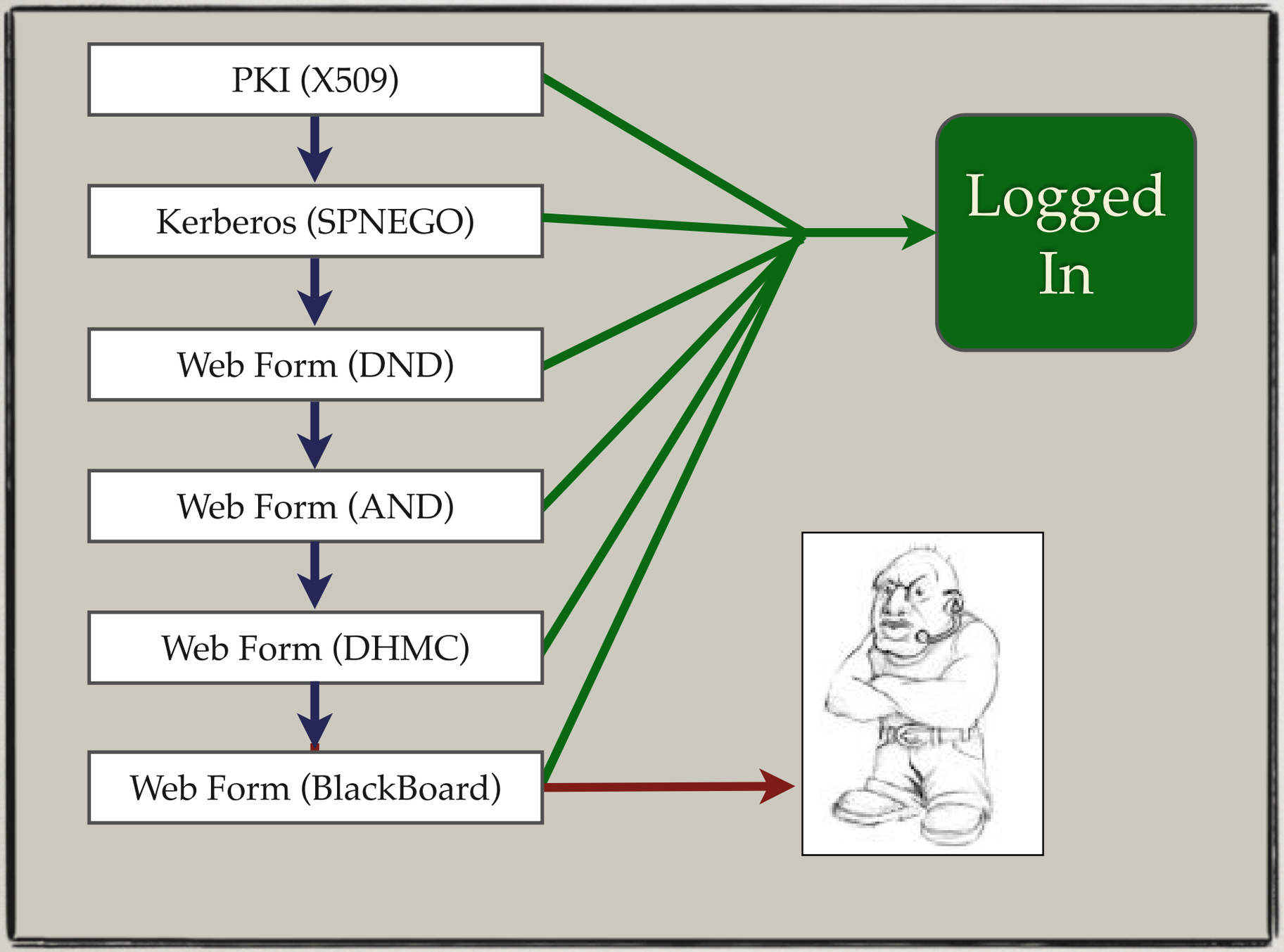
II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations



Authentication Handlers

Authentication handlers perform the actual steps to authenticate a user. The diagram above shows the current order of handlers.

Realms

Handler	Realm	authType
Dartmouth PKI	DARTMOUTH.EDU	PKI
Dartmouth SPNEGO	DARTMOUTH.EDU	SPNEGO
Dart Name Directory	DARTMOUTH.EDU	USERPASS
Alumni Name Directory	DARTMOUTH.ORG	USERPASS
DHMC Name Directory	HITCHCOCK.ORG	USERPASS
BlackBoard	BB.DARTMOUTH.EDU	USERPASS
??	??	??

Unique UIDs

Handler	Realm	UID
Dartmouth PKI	DARTMOUTH.EDU	
Dart SPNEGO	DARTMOUTH.EDU	
Dart Directory	DARTMOUTH.EDU	
Alumni Directory	DARTMOUTH.ORG	AL-
DHMC Directory	HITCHCOCK.ORG	DH-
BlackBoard	BB.DARTMOUTH.EDU	BB-
??	??	??

Specifying An Authentication Hanlder

- Additional parameter to the login URL
  - handler=AND
- Changes to the Credentials Class
- AuthHandlers ignore based on parameter
- Hard Requirement

- Alternative: using service registration

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

CAS XML Extensions

- Extend the Principal Class
- Modify CredentialsToPrincipalResolver
- Reconfigure deployerConfigContext.xml
- Add fields to the 2.0 protocol JSP file

CAS XML Extensions

- Extend the Principal Class
- Modify CredentialsToPrincipalResolver
- Reconfigure deployerConfigContext.xml
- Add fields to the 2.0 protocol JSP file

```
DartmouthPrincipal.java
DartmouthUsernamePasswordCredentialsToPrincipalResolver.java
PrincipalBearingCredentialsToDartPrincipalResolver.java
X509CertificateCredentialsToDartIdentifierPrincipalResolver.java

casServiceValidationSuccess.jsp
```

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran@DARTMOUTH.EDU</cas:user>
        <cas:uid>66035</cas:uid>
        <cas:did>HD1205K7</cas:did>
        <cas:affil>DART</cas:affil>
        <cas:authType>PKI</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS XML Extensions Client Support

- Apache
- Perl
- Java
- PHP
- Ruby

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

Authenticate Package

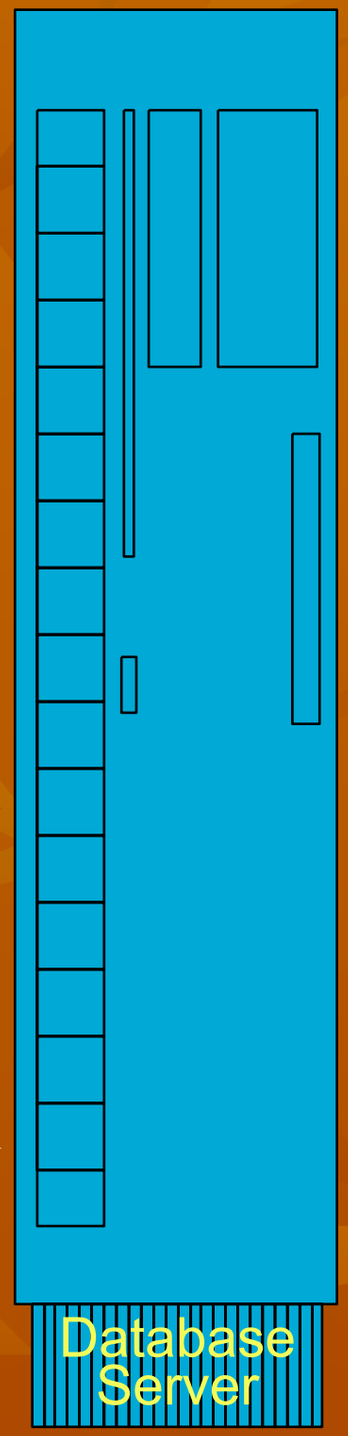
- Written in pl/sql
- Used by over 30 applications
- involved a DB pipe and external listeners
- Returned the username and dctsnum

Authentication Architecture Using AUTHENTICATE

Client

DBMS Pipe (port 913)

Kerberos Listener



Database Server

DND Listener

DBMS Pipe

DND Server

http://oracle-dev/dart/chico/authenticate.display_who

Oracle Application Server

mod_plsql (DAD

Authenticate v3

- Designed to be a Drop-in Replacement
- Started with Yale pl/sql client
- Added Cookies
  - One Cookie for all Oracle Apps
  - Encrypted user data (attributes, IP, timestamp, secret)
- Change in Application Flow
  - Call to Authenticate_v3 must happen before any content is written to client or redirect will fail

Oops...

How mod_plsql Works

- Apache module
  - Hooks in as a content handler
- Maps incoming URL to pl/sql proceedure
  - Parameters must match

```
http://oas.example.com/myfunction?foo=1

myfunction(int foo) {
   ...
}
```

Handling the Ticket Parameter

- CASTicketStripper Apache module
  - Removes the Ticket parameter from URL
  - Places Ticket value in Apache Environment
  - Hooks into Apache before mod_plsql
  - Written in Perl
- F5
  - Removes Ticket parameter from URL
  - Passes to IAS serves in Apache Environment
  - Written in TCL

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

Gotcha: Single Sign Off

- What does Signing off mean?
  - Local App? All Apps?
  - What is the user expecting?
- What is the user expecting?
- Worst case: Kerberos & PKI

Logout Solution

- Indicate status on all web pages
- Provide a local logout link
  - Kills local sessions
  - Redirects to Dartmouth logout script
- Dartmouth Logout Script
  - Includes Application name and link if passed in
  - Clear, Concise reminder to users
  - Link to CAS logout link

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

Clustering

- Terracotta: JVM level clustering
- JBossCache: Distributed Ticket Cache

Clustering

- Terracotta: JVM level clustering
- JBossCache: Distributed Ticket Cache

- Round-Robin DNS
- Load Balancer

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

The Greening of CAS

I. Multiple Identity Stores

II. CAS 2.0 XML Extensions

III. Integration in Oracle Applications

IV. Logout Best Practices

V. Clustering

VI. Handling Public Workstations

Public Workstations

- Default Session too long
- Moved all workstations to a special subnet
- CAS Session length shortened
- Reminders to quit browser
- eTokens

More Information

Project Website

http://dev.dartmouth.edu/projects/softdev/webAuth/

CAS v3

http://www.ja-sig.org/products/cas/

Shibboleth

http://shibboleth.internet2.edu/

Questions