SSO and ColdFusion using CAS

by Daniel Daugherty
daniel_cfug@danield.us.

Ageda

- What is SSO?
- Why use SSO?
- How does SSO work?
- Options for SSO?
- What is CAS?
- How to setup CAS?
- Connecting your CAS application to SSO?

What is SSO

- SSO stands for Single Sign-On
- What is Single Sign-On?
  - Wikipedia Definition:
    Single sign-on (**SSO**) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. **Single sign-off** is the reverse process whereby a single action of signing out terminates access to multiple software systems.

SSO pros/cons

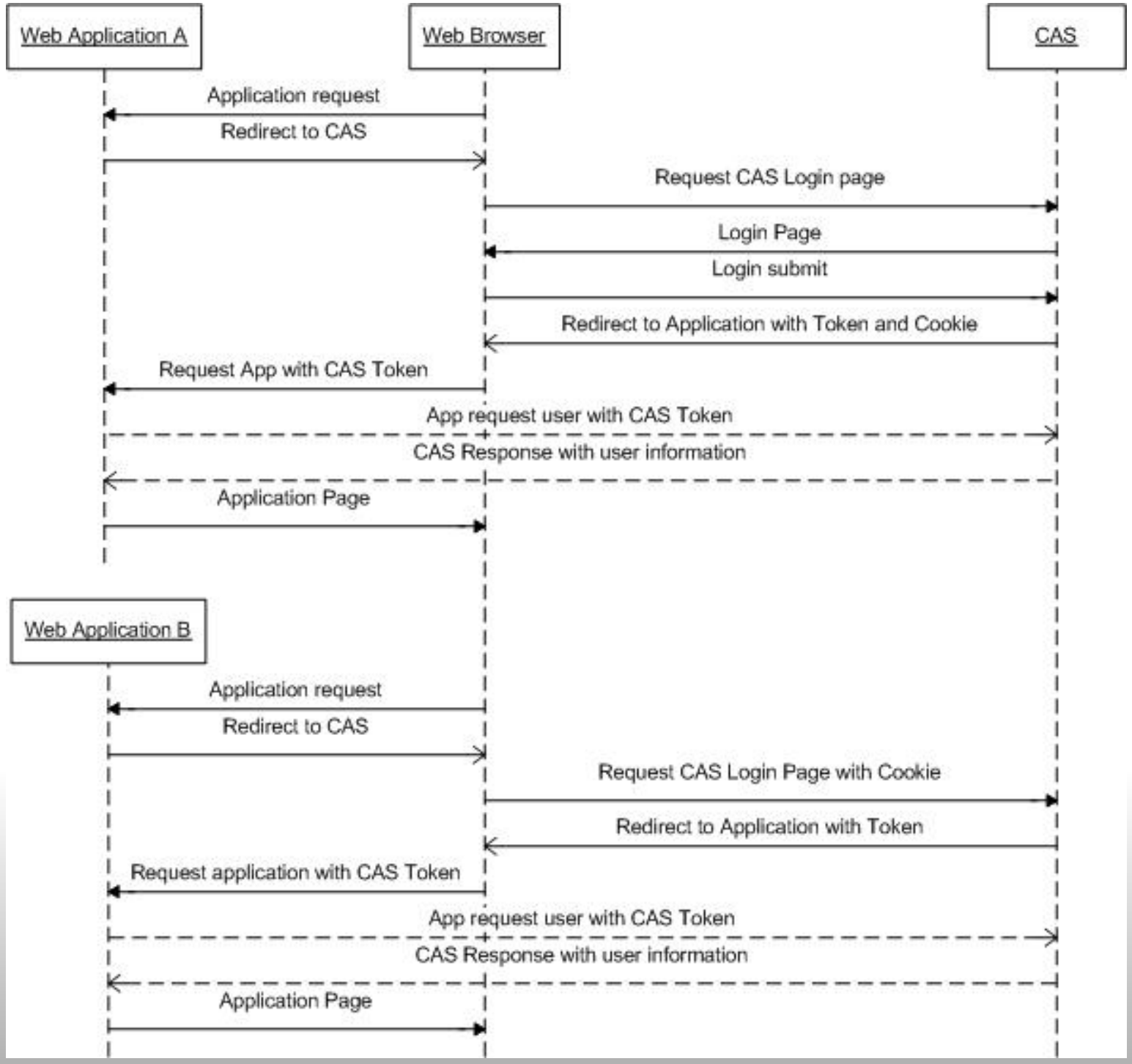
- Pros
  - Increased security single username and password.
  - Decreased user account support and maintenance.
  - Increased ease of use.
  - Remote authentication
  - Less code to maintain.
  - Less passwords to remember.
- Cons
  - Decreased security single username and password.
  - One key to the entire castle

Examples of SSO

- iGoogle, Gmail, Google Reader, ...
- Yahoo Mail, My Yahoo, ...
- Windows Network

Ways to Authentication Users with SSO

- Web based form
- HTTP Basic Auth
- Windows Authentication
  - NTLM
  - Kerberos
  - SPNEGE
- Smart Card
- X.509 Certificates
- OTP Token : RSA Secure-ID
- Bio Metric
- .....


Web Application A
Web Browser
CAS
Application request
Redirect to CAS
Request CAS Login page
Login Page
Login submit
Redirect to Application with Token and Cookie
Request App with CAS Token
App request user with CAS Token
CAS Response with user information
Application Page
Web Application B
Application request
Redirect to CAS
Request CAS Login Page with Cookie
Redirect to Application with Token
Request application with CAS Token
App request user with CAS Token
CAS Response with user information
Application Page

Introducing JA-SIG CAS

What is CAS?
CAS is an authentication system originally created by Yale University to provide a trusted way for an application to authenticate a user. CAS became a JA-SIG project in December 2004

What does CAS stand for?
Central Authentication Service

CAS requirements

CAS 3.X requires

Java 1.5 or higher
J2EE 1.3
JSP 2.0 support

CAS supported clients

- CFML
- Java
- JSP
- Ruby
- PHP
- Perl
- .Net C#
- JSR-168 - JAVA Portal
- WebObjects
- .....
- ANY Language that can do HTTP request and parse HTML.

CAS install setup

- Download CAS bundle.
- Determine what you will authenticate against
- Configure CAS for your chosen auth provider
  - Manual update and configure cas-server-webapp-3.3.war
  - OR use Maven to Build war package.

For JDBC used in this presentation
See direction on
http://www.ja-sig.org/wiki/display/CASUM/Using+JDBC+for+Authentication

DEMO

Trouble Shooting CAS

- Authinticate directly to the CAS server http[s]://yourcasserver/cas/login
- Use a network sniffer to see traffic.
  - Check traffic between browser and CAS
    - Look for CAS cookies
    - Look for redirect to application with token
  - Check traffic between browser and application
    - Look for redirect to CAS server
    - Look CAS url token being sent
  - Check traffic between application server and CAS server.
    - Look for call to serviceValidate with valid ticket.
- Enable Debug on CAS and Check logs.

What about Authorization

CAS is a Authintication system it does not perform Authorization checks.

Authorization is the responsibility of the individual applications.

Some SSO systems such as CA Siteminder can perform Authorization test but most do not.

CAS follows the "do one thing and do that well" principle.

CAS and User Management

- CAS currently does not do user management.
- If authentication system is also used for computer logins then that system will manage passwords etc.
- If you are using database then you will probably want to build or use an existing user management.

Common user management items

- create/disable account
- change/expire password

Resources

Wikipedia Single_sign-on
- http://en.wikipedia.org/wiki/Single_sign-on

JA-SIG CAS
- Home
- http://www.ja-sig.org/products/cas/
- User Manual
- http://www.ja-sig.org/wiki/display/CASUM/Home
- Clients
- http://www.ja-sig.org/products/cas/client/libraries/index.html
- CAS JDBC setup

http://www.ja-sig.org/wiki/display/CASUM/Using+JDBC+for+Authentication

Resources 2

Network sniffing tools

- WireShark - formerly Ethereal: http://www.wireshark.org/
- JRUN SNIFFER / Proxy
- Eclipse TCP/IP Proxy

Questions?

daniel_cfug@danield.us