

CAS

explained, deployed, extended at Pepperdine
University

Speaker Background

- Not a Java Architectures “maven”
- Educational technologist, with system administrator background with a lot of work in information security since 2k4.
- “Perfect” for implementing CAS
- And you?

University Environment

- Private, Christian University
- 8,500 Students - half are fully-employed
- 4 campus WAN in SoCal
- 5 International campuses across Internet

CAS Goals

- Lower integration costs
- Increase ease of use
- Reduce the cost of password reset
- and CAS will be good for security

CAS Protocol

- Overview from the browser & client perspective
- 4 “live” slides

CAS ServiceValidate

- GET ticket to /cas/serviceValidate
- e.g.:
 - GET /cas/serviceValidate?service=https://networkid.pepperdine.edu/google/signin.aspx&ticket=ST-1823-pE4kQZqqNscRYh3nFAbf-pcas

CAS samlValidate















- POST ticket to /cas/samlValidate
- POST /cas/samlValidate?TARGET=http%3A%2F%2Fedns-test01.pepperdine.edu%2FcastestUnblock.phpWTcZBar-kXaYWxcCx5mvIR-LXJw2kmVj8CZd5QO6dOZFTfcGsgzKOfEUISSsPQX2OIppNPjbttyEC5ETw2%26t%3d4ef66275


```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <samlp:Request xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
MajorVersion="1"
MinorVersion="1" RequestID="_192.168.16.51.1024506224022"
IssueInstant="2010-03-01T17:03:44.022Z">
      <samlp:AssertionArtifact>
        ST-1-u4hrm3td92cLxpCvrjyl-pcas
      </samlp:AssertionArtifact>
    </samlp:Request>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```


CAS Services

👁️ Live Demo of Service Management

Manage Services

Service Name	Service Url	Enabled	Can Proxy	SSO		
CAS Test	http://edns-test01.pepperdine.edu/castest*.php	✓	✓	✓	 edit	 d
Kim's testing	http://137.159.16.97/castest?.php	✓	✓	✓	 edit	 d
Network ID Test	http://tnetworkid.pepperdine.edu/**	✓	✓	✓	 edit	 d
Secure Network ID Test	https://tnetworkid.pepperdine.edu/**	✓	✓	✓	 edit	 d
Services Management	https://edns-test01.pepperdine.edu:9443/cas/**	Status	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Allow	 edit	 d
Waxwood	http://waxwood.pepperdine.edu/**	Attributes	<ul style="list-style-type: none">givenNamedistinguishedNamemailemployeeIDdisplayNamesndescriptionmemberOf		 edit	 d
...	...				 ...	 ...

 add new service

CAS Deployment

- Set-up Tomcat
 - dev, test & production tiers/instances
 - log valve (to get logs for bare tomcats)
- Add CAS
 - Customize `deployerConfigContext.xml`
 - Build with maven
 - Drop `cas.war` in tomcat webapp folder

Tomcat Architecture

- Single Tomcat Binary, multiple configuration instances

```
export CATALINA_HOME=/usr/local/tomcat
export CATALINA_BASE=/usr/local/tomcat-test
```

- e.g., Limited hardware for separating tiers, easier tomcat upgrade

- Brittain & Darwin (2007). Tomcat: The Definitive Guide, 2nd Ed. p.40

- Mac OS/X Server – service control

- Start & Stop instances independently

- Brittain & Darwin (2007). Tomcat: The Definitive Guide, 2nd Ed. p.32

CAS Maintenance

- for customizations & version updates --
- Maintain a local folder tree of changed files
 - deployerConfigContext.xml
 - modified gui .jsp or .properties files
- Merge these changes with the CAS version codebase you specify in POM.xml using Maven
- Deploy the updated cas.war

Maven Live

- We keep our tree of changed files in svn
- I've copied them out here in my computer so we can edit them
- We'll look at the POM.xml and do an edit +build

CAS Extension

- Our Evil Plan
- Hook CAS authentication after login success
- Check for enrollment in password reset
- If not, send them to the password reset enrollment instead of their app! >:)
- Let's see how this works!

Bean call in `deployerConfigContext.xml` (referencing an external instance specific url config file)

```
<!--  
    Local action for the Spring Web Flow that checks the Network Id Profile.  
-->  
<bean id="networkIdProfileCheck" class="edu.pepperdine.cas.web.flow.NetworkIdProfileCheck">  
    <constructor-arg index="0" ref="networkIdWebServiceUrl" />  
    <constructor-arg index="1" ref="networkIdWebServiceSharedSecret" />  
    <constructor-arg index="2" ref="networkIdProfileApplicationUrl" />  
    <property name="enabled" ref="enableNetworkIdProfileApplicationRedirect" />  
</bean>
```


CAS Availability Strategy

- VM constructed from backup of CAS server
- Refreshed after major changes & deployed to two standby servers (multi-use)
- Manual cutover

Your CAS Client App

- Easy with a CAS client library!
- Otherwise, just implement the CAS protocol with your code (don't forget sign-out!)
- To convert an existing cookie-session based application:
 - Set the cookie only after your CAS library confirms authentication (and any required attributes).
 - Invalidate the cookie when your application receives the CAS server single sign-out call.

Machines and ports blocked for security reasons

Data last updated Sun, 07 Mar 2010 19:33:27 -0800

Time_blocked	Time_unblocked	Status	HEAT	Reason	IP	MAC	WINS
2010-03-05 14:10:40	2010-03-05 15:24:37	Unblocked MAC at CampusManager for Copyright		infringe	137.159.135.66	0026bb134bc3	
2010-03-05 13:47:12		Blocked MAC at CampusManager for Malware		bot	137.159.153.178	001a73b24b70	
2010-03-05 12:40:40	2010-03-05 15:21:47	Unblocked MAC at CampusManager for Malware		bot	137.159.155.134	0021008d3ab7	
2010-03-04 07:32:11		Blocked MAC at CampusManager for Copyright		infringe	137.159.157.16	001e641d8a50	
2010-03-04 07:32:06		Blocked MAC at cr-pcc		bot	137.159.189.187	041e649ab36c	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.249.187	00904b732a1e	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.149.134	0014a5361a1c	
2010-03-03 00:11:32		Blocked MAC at CampusManager for Rogue_DHCP		dhcprogue	137.159.117.64	001d095fb4de	

Reason codes:

- bot:** **Problem:** Computer under control of criminals, for stealing information and/or attacking other computers.
Reason: Malware has compromised computer.
Fix: Reformat, fixmbr, reinstall O/S and restore data from backup; user must change passwords.
- dhcprogue:** **Problem:** Computer is handing out non-University DHCP server or bridging University DHCP service, causing service issues for other users.

Original App

Machines and ports blocked for security reasons

Welcome Mister Test

Data last updated Sun, 07 Mar 2010 19:33:27 -0800

Time_blocked	Time_unblocked	Status	HEAT	Reason	IP	MAC	WINS
2010-03-05 14:10:40	2010-03-05 15:24:37	Unblocked MAC at CampusManager for Copyright		infringe	137.159.135.66	0026bb134bc3	
2010-03-05 13:47:12		Blocked MAC at CampusManager for Malware		bot	137.159.153.178	001a73b24b70	
2010-03-05 12:40:40	2010-03-05 15:21:47	Unblocked MAC at CampusManager for Malware		bot	137.159.155.134	0021008d3ab7	
2010-03-04 07:32:11		Blocked MAC at CampusManager for Copyright		infringe	137.159.157.16	001e641d8a50	
2010-03-04 07:32:06		Blocked MAC at cr-pcc		bot	137.159.189.187	041e649ab36c	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.249.187	00904b732a1e	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.149.134	0014a5361a1c	
2010-03-03 00:11:32		Blocked MAC at CampusManager for Rogue_DHCP		dhcprogue	137.159.117.64	001d095fb4de	

Reason codes:

bot: **Problem:** Computer under control of criminals, for stealing information and/or attacking other computers.

Authenticated App

Unblock Page!

Kim Cary, you are authorized to unblock computers!

Data last updated Sun, 07 Mar 2010 19:33:27 -0800

Time_blocked	Time_unblocked	Status	HEAT	Reason	IP	MAC	WINS	
2010-03-05 14:10:40	2010-03-05 15:24:37	Unblocked MAC at CampusManager for Copyright		infringe	137.159.135.66	0026bb134bc3		
2010-03-05 13:47:12		Blocked MAC at CampusManager for Malware		bot	137.159.153.178	001a73b24b70		Unblock
2010-03-05 12:40:40	2010-03-05 15:21:47	Unblocked MAC at CampusManager for Malware		bot	137.159.155.134	0021008d3ab7		
2010-03-04 07:32:11		Blocked MAC at CampusManager for Copyright		infringe	137.159.157.16	001e641d8a50		Unblock
2010-03-04 07:32:06		Blocked MAC at cr-pcc		bot	137.159.189.187	041e649ab36c		Unblock
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.249.187	00904b732a1e		Unblock
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.149.134	0014a5361alc		Unblock
2010-03-03 00:11:32		Blocked MAC at CampusManager for Rogue_DHCP		dhcprogue	137.159.117.64	001d095fb4de		Unblock

Authorized App Content

Unblock Page!

Mister Test, you are not authorized to unblock computers!

Data last updated Sun, 07 Mar 2010 19:33:27 -0800

Time_blocked	Time_unblocked	Status	HEAT	Reason	IP	MAC	WINS
2010-03-05 14:10:40	2010-03-05 15:24:37	Unblocked MAC at CampusManager for Copyright		infringe	137.159.135.66	0026bb134bc3	
2010-03-05 13:47:12		Blocked MAC at CampusManager for Malware		bot	137.159.153.178	001a73b24b70	
2010-03-05 12:40:40	2010-03-05 15:21:47	Unblocked MAC at CampusManager for Malware		bot	137.159.155.134	0021008d3ab7	
2010-03-04 07:32:11		Blocked MAC at CampusManager for Copyright		infringe	137.159.157.16	001e641d8a50	
2010-03-04 07:32:06		Blocked MAC at cr-pcc		bot	137.159.189.187	041e649ab36c	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.249.187	00904b732a1e	
2010-03-04 07:31:59		Blocked MAC at CampusManager for Malware		bot	137.159.149.134	0014a5361a1c	
2010-03-03 00:11:32		Blocked MAC at CampusManager for Rogue_DHCP		dhcprogue	137.159.117.64	001d095fb4de	

[Raw CSV file](#)

Reason codes:

bot: **Problem:** Computer under control of criminals, for stealing information and/or

Authenticated/Unauthorized

Goals

- Lower cost of integration
 - still working to show integrators it's worth doing things differently
- Ease of use -- absolutely!
- Reduce the cost of password reset.
 - Too early (implemented pw reset enrollement check in Jan 2010) to tell
- Security
 - Fewer apps have passwords!

Integration Thus Far

- Library Databases (ez-proxy)
- iTunesU (via connector)
- Anywhere Storage (Xythos)
- Sakai (LMS)
- Google Apps/Mail (via connector)
- Web Content Management System (Omniupdate)
- Voice Thread
- IT Blogs & Change Control
- Event submission forms
- Institutional Effectiveness Reporting Apps
- Network ID (password reset portal)

Integration – Pending

- Peoplesoft Portal (tested, waiting)
- ClearPass Apps (waiting on me :)
 - Outlook Web Access
 - Kronos Time Accounting
- Simpler Systems (var integration pending)

Other

- Inspektr database
 - Audit trail and throttling
 - Use Stats
- Future
 - ClearPass
 - High Availability
- Questions?