

Get Smart! About RIA Security

by Brian Rinaldi

www.cfunitd.com

About This Presentation

A. Originally submitted by Rob Gonda. I adhere to the general intent of his concept with a significant exception:

•There is no bullet-proof solution!

B. **Intended Audience: Intermediate Level**

C. You should be familiar with building RIA's using either Ajax or Flex, though we will generally focus on Flex.

2

June 18 - 21, 2008

www.cfunitd.com

Who Am I?



3

June 18 - 21, 2008

www.cfunitd.com

- A. Adobe Community Expert
- B. Flex Champion
- C. Boston ColdFusion User Group Manager
- D. Organizer of Flex Camp Boston (Dec. 2007)
- E. Creator of the Illudium PU-36 Code Generator open-source project
- F. Frequent author to publications including Fusion Authority Quarterly Update, Adobe Edge, Sitepoint, ColdFusion Weekly Podcast
- G. Blog - RemoteSynthesis.com
- H. ColdFusion Open-Source List
- I. Weekly ColdFusion Open-Source Update

A Multi-layer Approach to Security

- A. You, the developer, are a
- B. agent for CONTROL fighting
- C. the agents of KAOS!
- D. Much like the entrance to the
- E. CONTROL headquarters, you need to implement
- F. many secure doors. Your goal is to make it as
- G. difficult as possible to get in.



4

June 18 - 21, 2008

www.cfunitd.com

The Secure Doors (or Layers)

- A. We will discuss 4 "layers" today for protecting RIAs:
- B. Roles-based security for remote methods
- C. Domain security for remote methods
- D. HTTPS
- E. Data encryption

5

June 18 - 21, 2008

www.cfunitd.com

Tools for Intercepting Data

- A. **Service Capture**
 - <http://kevinlangdon.com/serviceCapture/>
 - Can deserialize and display all Flash Remoting or AMF traffic
- B. **Charles**
 - <http://www.xk72.com/charles/>
 - Can capture HTTP/SSL communication
- C. **Firebug**
 - <http://www.getfirebug.com/>
 - Integrates with Firefox
 - Monitor network activity

6

June 18 - 21, 2008

www.cfunitd.com

Roles-based Security (Layer 1)

- A. The most basic layer and yet often
- B. overlooked.
- C. Create a list of core user roles
 - Not logged in could be just "user"
- D. Determine access to API based upon these roles
 - Err on the side of more restrictive



7

June 18 - 21, 2008

www.cfunitd.com

Implementing Roles-Based Security: ColdFusion Wrapper

- A. Change the included template name
- B. Modify Eclipse/Flex Builder project settings
- C. Run Project > Clean...
- D. Eclipse will generate a CFM that will work with your application.cfc to handle session-based logins.

<http://www.kylehayes.info/blog/index.cfm/2007/3/5/Flex-HTMLTemplate-filetype-to-CFM-instead-of-HTML>

8

June 18 - 21, 2008

www.cfunitd.com

Implementing Roles-Based Security: Remote Methods

- A. **<cflogin>**
- B. Manage user logins and roles.
- C. **<cffunction>**
- D. Remote proxy component
- E. Set allowable roles via the roles attribute

<http://www.kylehayes.info/blog/index.cfm/2007/3/5/Flex-HTMLTemplate-filetype-to-CFM-instead-of-HTML>

9

June 18 - 21, 2008

www.cfunitd.com

Domain-based Security (Layer 2)

- A. Flex
 - Crossdomain.xml and Cross Domain permissions
- B. Ajax
 - ColdFusion 8 Ajax Security

10

June 18 - 21, 2008

www.cfunitd.com

Cross-domain Permissions in Flex

- A. Specifies what domains are allowed to call data via a SWF

```
<?xml version="1.0"?><!-- http://www.foo.com/crossdomain.xml -->
<cross-domain-policy>
  <allow-access-from domain="www.friendOfFoo.com"/>
  <allow-access-from domain="*.foo.com"/>
  <allow-access-from domain="105.216.0.40"/>
</cross-domain-policy>
```

11

June 18 - 21, 2008

www.cfunitd.com

ColdFusion 8 Ajax Security Tools

- A. **VerifyClient**
- B. function (verifyClient()) or attribute on **<cffunction>** (verifyclient="true")
- C. client or session management must be enabled
- D. **JSON Prefixes**
- E. global via ColdFusion Administrator setting
- F. via **<cfapplication>** or Application.cfc
- G. via **<cffunction>** attribute

http://www.adobe.com/devnet/coldfusion/articles/ajax_security.html

12

June 18 - 21, 2008

www.cfunitd.com

HTTPS (Layer 3)

- A. "Because a SWF file running within a browser uses the browser for almost all of its communication with the server, it can take advantage of the browser's built-in SSL support. This lets communication between the SWF file and the server be encrypted.
- H. Furthermore, the actual bytes of the SWF file are encrypted while they are being loaded into the browser. Thus, by playing a SWF file within an SSL-enabled browser through an HTTPS connection with the server, you can ensure that the communication between Flash Player and the server is encrypted and secure."



Cone of Silence

http://livedocs.adobe.com/flex/3/html/help.html?content=security2_14.html#141403

13

June 18 - 21, 2008

www.cfunitd.com

Data Encryption (Layer 4)

- A. Flex
 - One-Way Encryption
 - § Corelib Library
 - Two-Way Encryption
 - § as3Crypto
- B. Ajax
 - One-Way Encryption
 - § JavaScript
 - Two-Way Encryption
 - § RSA Library



14

June 18 - 21, 2008

www.cfunitd.com

Implementing One-Way Data Encryption in Flex

- A. Encrypt protected passwords via AES using Corelib
- B. One-way hashing of data that you do not need to decrypt
- C. To verify encrypted password
 - Encrypt the password
 - Pass encrypted password
 - Compare to stored version

15

June 18 - 21, 2008

www.cfunitd.com

Two-Way Encryption in Flex

- A. You can access RSA libraries via AS3Crypto open-source library
- B. As of the writing of this presentation I could not get data encrypted in Flex to decrypt in CF.

16

June 18 - 21, 2008

www.cfunitd.com

Additional Resources

- A. ColdFusion 8 Ajax Security Functions - http://www.adobe.com/devnet/coldfusion/articles/ajax_security.html
- B. JavaScript - <http://www.fourmilab.ch/javascript/>
- C. RSA Implementation - <http://home.versatel.nl/MAvanEverdingen/Code/>
- D. CF7 encryption additions : <http://www.petefreitag.com/item/222.cfm>
- E. AS3 cryptography library (RSA) - <http://crypto.hurlant.com/>
- F. AS3 Core Lib (SHA256) - <http://code.google.com/p/as3corelib/>
- G. Issues with converting encryptions between cf and flex - <http://www.jeffryhouser.com/index.cfm/2007/12/6/Encrypt-in-Flex-and-Decrypt-in-ColdFusion>
- H. Flex and Encryption - http://blogs.oreilly.com/cgi-bin/mt/mt-search.cgi?tag=encryption&blog_id=34&includeBlogs=34
- I. Secure SWF - http://www.adobe.com/devnet/flashplayer/articles/secure_swf_apps.html
- J. OAuth - <http://oauth.net/>
- K. Public Key Encryption for Dummies - <http://www.networkworld.com/news/tech/0517tech.html>
- L. SWF Decompilers - <http://www.decompiler-swf.com/> <http://code.google.com/p/flash-decompiler/>

17

June 18 - 21, 2008

www.cfunitd.com

Questions?

- A. email: brian.rinaldi@gmail.com

18

June 18 - 21, 2008

www.cfunitd.com