



MAX 2006 Beyond Boundaries



Peter Martin
Understanding Security in Flex
and Flash
Adobe Consultancy

2006 Adobe Systems Incorporated. All Rights Reserved. 1

Who am I?



- Peter Martin
- Technical Architect with Adobe Consulting
- Rich Internal Applications, EMEA
- Edinburgh, Scotland
- Background
 - Enterprise software development
 - J2EE
- Flex Community
 - FlexUnit Ant Task
 - FDS Plugin for Eclipse WTP
 - EJB and Flex Integration
 - Cairngorm Security

2006 Adobe Systems Incorporated. All Rights Reserved. 2

Agenda

- Introduction
- Server Security
 - J2EE Security
 - FDS Security
- Client Security
 - Flash Security
 - Flex Security
- Sample Application

2006 Adobe Systems Incorporated. All Rights Reserved. 3

Introduction

What are we going to cover?



2006 Adobe Systems Incorporated. All Rights Reserved. 4

What are we going to cover?

- Authentication
- Authorization
- Confidentiality (communication links)

2006 Adobe Systems Incorporated. All Rights Reserved. 5

What is Authentication?

“validate a user’s identity based on their credentials”

2006 Adobe Systems Incorporated. All Rights Reserved. 6

What is Authorization?

“determine whether the identity of the user has the necessary privileges to request the resource”

2006 Adobe Systems Incorporated. All Rights Reserved. 7

What is Confidentiality?

“ensuring that information is accessible only to those authorized to have access”

International Organization for Standardization (ISO)

2006 Adobe Systems Incorporated. All Rights Reserved. 8

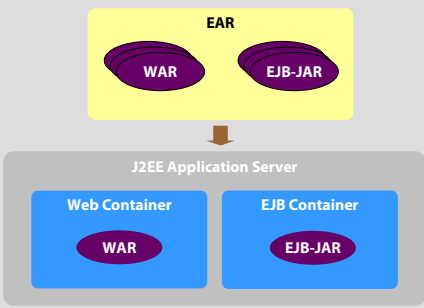
J2EE Security – A Quick Primer

How is a J2EE application deployed?
How is FDS related to J2EE?
What is the J2EE security model?



2006 Adobe Systems Incorporated. All Rights Reserved. 9

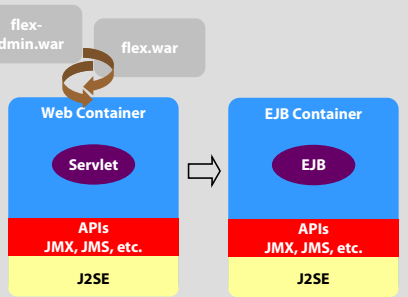
How is a J2EE application deployed?



2006 Adobe Systems Incorporated. All Rights Reserved. 10

How is FDS related to J2EE?

- FDS built on J2EE



2006 Adobe Systems Incorporated. All Rights Reserved. 11

What is the J2EE security model?

- Role-based
- Declarative Security
- Programmatic Security
- Standards only go so far, for example:
 - the Servlet specification doesn't define logout
- Implementations & extensions vendor specific

2006 Adobe Systems Incorporated. All Rights Reserved. 12

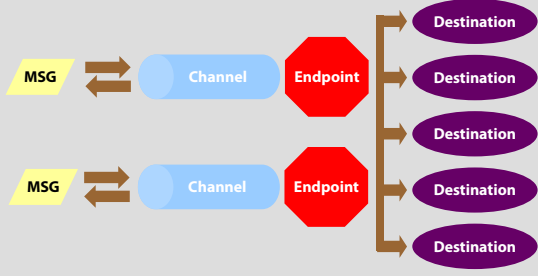
FDS Security

What are destinations, channels and endpoints?
 How do you secure an endpoint?
 How do you secure a destination?



2006 Adobe Systems Incorporated. All Rights Reserved. 13

What are destinations, channels and endpoints?

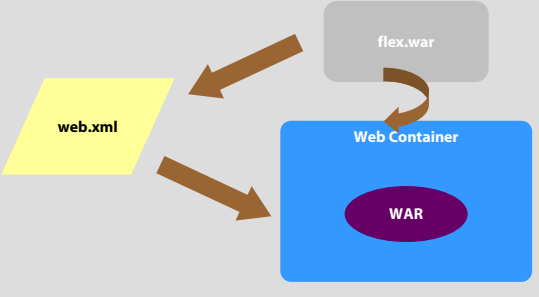


The diagram illustrates the message flow in a service-oriented architecture. It starts with a yellow 'MSG' box on the left. Two arrows point from the MSG to a blue 'Channel' box. From the Channel, two arrows point to a red octagonal 'Endpoint' box. From the Endpoint, four arrows point to four purple oval 'Destination' boxes stacked vertically on the right.

2006 Adobe Systems Incorporated. All Rights Reserved. 14

How do you secure an endpoint?

- Basic Authentication



The diagram shows the deployment process for an endpoint. A yellow 'web.xml' file and a grey 'flex.war' file are shown with arrows pointing to a blue 'Web Container' box. Inside the Web Container is a purple oval labeled 'WAR'.

2006 Adobe Systems Incorporated. All Rights Reserved. 15

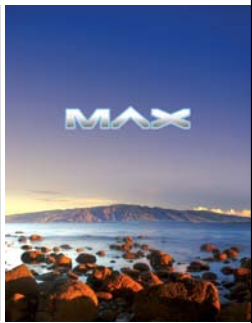
How do you secure a destination?

- Basic Authentication
- Custom Authentication

2006 Adobe Systems Incorporated. All Rights Reserved. 16

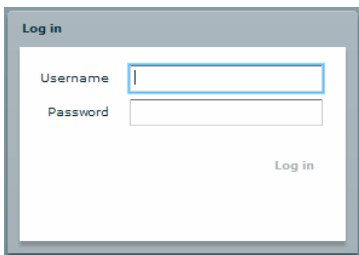
Custom Authentication

What is custom authentication?
 How is the user authenticated?
 How do you set credentials?



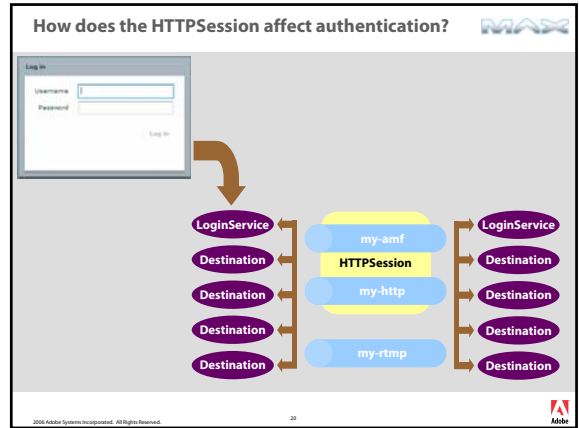
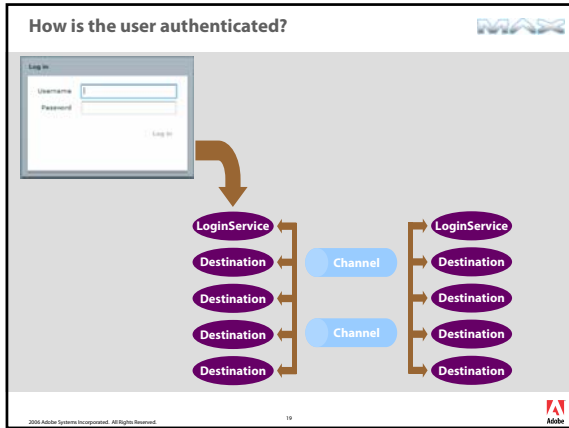
2006 Adobe Systems Incorporated. All Rights Reserved. 17

What is custom authentication?



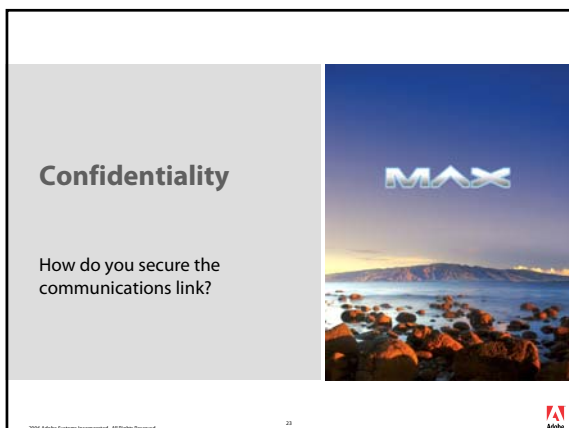
The screenshot shows a 'Log in' form with two input fields: 'Username' and 'Password'. A 'Log in' button is located at the bottom right of the form.

2006 Adobe Systems Incorporated. All Rights Reserved. 18



- ### How do you set credentials?
- Accessing secure destinations:
 - AbstractService (RemoteObject, WebService)
 - HTTPService
 - MessageAgent (Consumer, Producer)
 - DataService
 - setCredentials(username : String, password : String);
 - logout();
- The Adobe logo and page number 21 are visible at the bottom.

- ### What about Cairngorm?
- Cairngorm 2.1
 - Security support added to ServiceLocator
 - setCredentials(username : String, password : String);
 - logout();
 - Go see Steven Webster's talk on "Delivering RIA Solutions with Cairngorm 2"
- The Adobe logo and page number 22 are visible at the bottom.



- ### How do you secure the communications link?
- Secure Sockets Layer
 - A cryptographic protocol that provides secure communications
 - endpoint authentication
 - communications privacy
 - Can be used with HTTP
 - Can be used with RTMP
 - SSL is based on the PKI (public key infrastructure)
 - Requires a certificate on the server
- The Adobe logo and page number 24 are visible at the bottom.

What SSL is not?

- SSL doesn't offer persistent security

"Hello World" → ZZZZZ CNHBF MTPIH AWNCP SDHGS QEUUE → "Hello World"

2004 Adobe Systems Incorporated. All Rights Reserved. 25

Flash Security

What is relevant to a Flex developer?



2004 Adobe Systems Incorporated. All Rights Reserved. 26

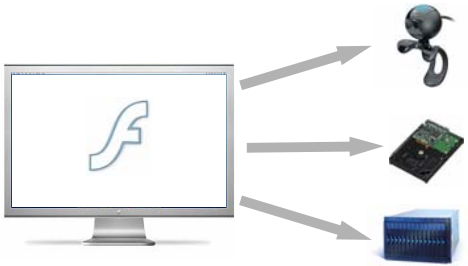
What is relevant to a Flex developer?

- Safe by default
- ActionScript very similar to JavaScript
 - except compiled byte code doesn't suffer from XSS vulnerabilities
- Depends on interactions between three parties:
 - User
 - Websites
 - Developer

2004 Adobe Systems Incorporated. All Rights Reserved. 27


What can the user control?


- The Flash Player executes on the client's computer...



2004 Adobe Systems Incorporated. All Rights Reserved. 28

What can the website control?

- The Flash Player loads the RIA from a web server...
 

<https://www.domainA.com/MyApplication/Main.swf>
- The RIA can load data from another domain...
 

https://www.domainB.com/stocks_quotes.xml

2004 Adobe Systems Incorporated. All Rights Reserved. 29

What can the developer control?


- The Flash Player executes the RIA within its security environment...



2004 Adobe Systems Incorporated. All Rights Reserved. 30

Flex Security

What role does Flash play?
 What about FDS?
 Is there anything else?



2006 Adobe Systems Incorporated. All Rights Reserved. 31

What role does Flash play?

- The Flex framework is built on Flash
- A Flex application is comprised of MXML and ActionScript files
- A Flex application is compiled into a binary SWF file
- A Flex application executes within the Flash Player
- The Flash security model is inherent with Flex

2006 Adobe Systems Incorporated. All Rights Reserved. 32

What about FDS?

- Your Flex application can call Flex Data Services
 - which are deployed on a J2EE application server
 - and inherit from the J2EE security model
- You can create a custom login page in Flex
- You use Flex to set the user credentials and to logout

2006 Adobe Systems Incorporated. All Rights Reserved. 33


Is there anything else?

- How do we surface user permissions?

2006 Adobe Systems Incorporated. All Rights Reserved. 34

Sample Application

Use Cases
 Deployment
 The Code

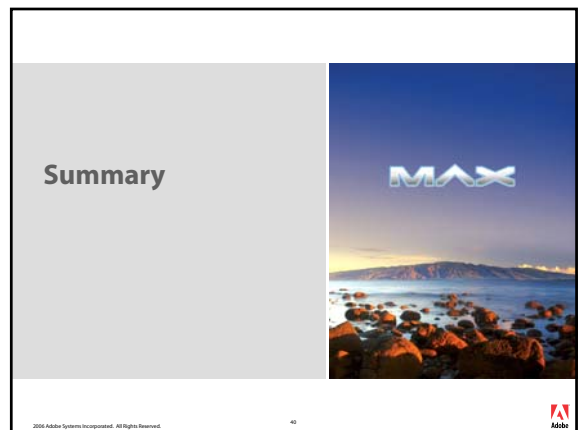
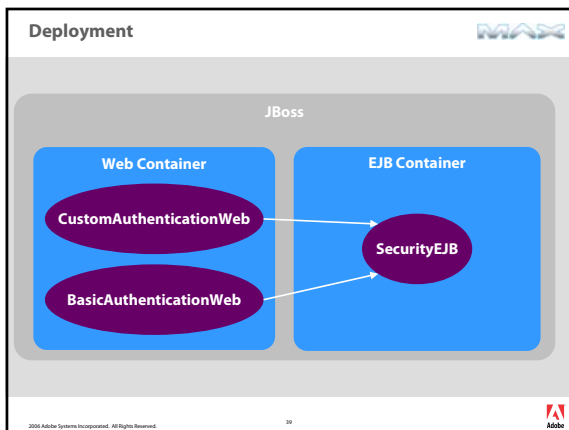
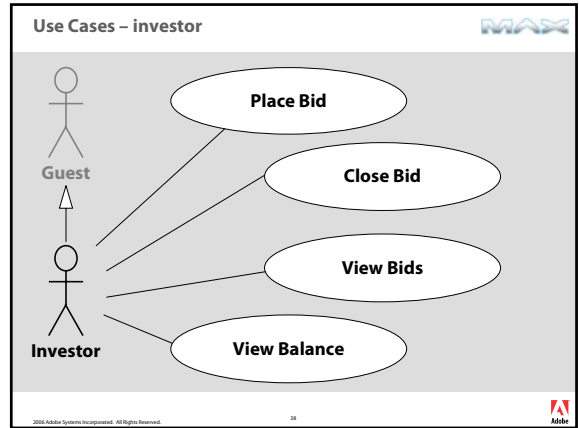
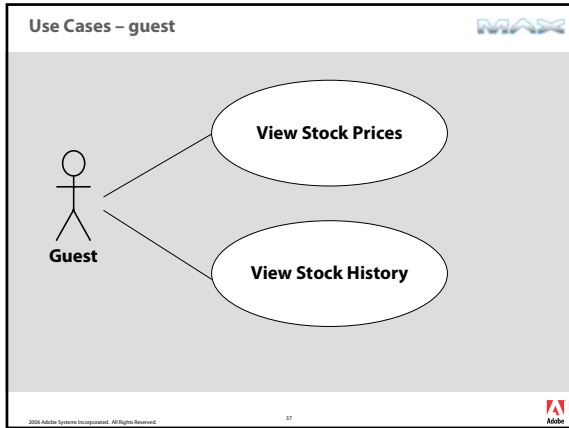


2006 Adobe Systems Incorporated. All Rights Reserved. 35

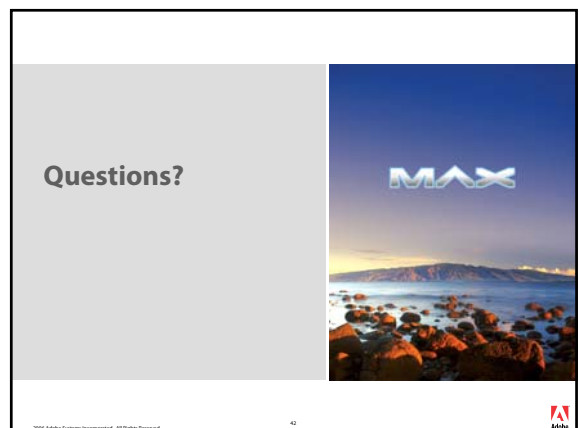
Flex Spread Betting

<<insert screen shot>>

2006 Adobe Systems Incorporated. All Rights Reserved. 36



- ### Summary
- Security is a broad subject
 - How authentication, authorization and confidentiality differ
 - The relationship between Flex, Flash, FDS and J2EE
 - Covered the different ways of securing a Flex application
 - Looked at implementing a custom login form
 - A quick look at a sample application
- 2006 Adobe Systems Incorporated. All Rights Reserved. 41



Better by Adobe.™