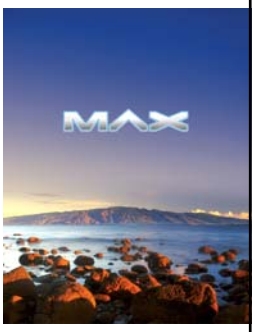
MAX 2006
Beyond Boundaries

Peter Martin

Understanding Security in Flex and Flash

Adobe Consultancy



Who am I?

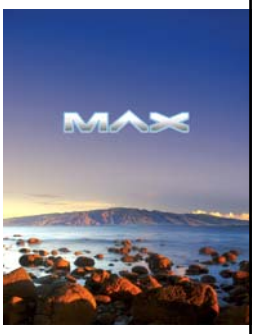
- Peter Martin
  - Technical Architect with Adobe Consulting
  - Rich Internal Applications, EMEA
  - Edinburgh, Scotland
- Background
  - Enterprise software development
  - J2EE
- Flex Community
  - FlexUnit Ant Task
  - FDS Plugin for Eclipse WTP
  - EJB and Flex Integration
  - Cairngorm Security

Agenda

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

Introduction

What are we going to cover?



What are we going to cover?

- Authentication
- Authorization
- Confidentiality (communication links)

What is Authentication?

"validate a user's identity based on their credentials"

What is Authorization?

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

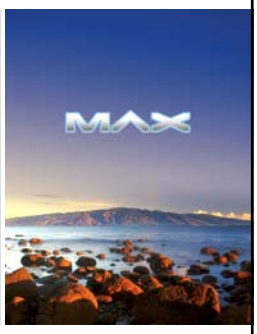
What is Confidentiality?

"ensuring that information is accessible only to those authorized to have access "

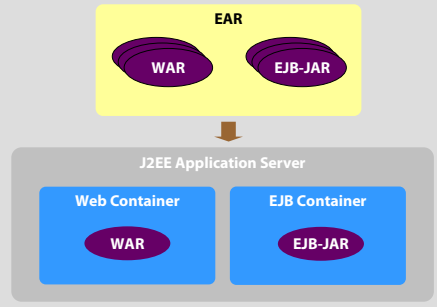
International Organization for Standardization (ISO)

J2EE Security – A Quick Primer

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

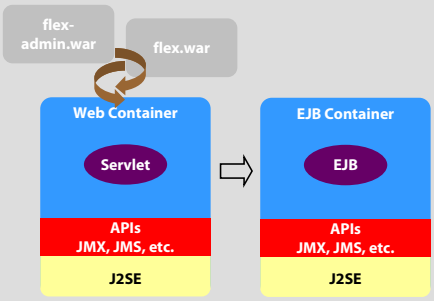


How is a J2EE application deployed?



How is FDS related to J2EE?

- FDS built on J2EE



What is the J2EE security model?

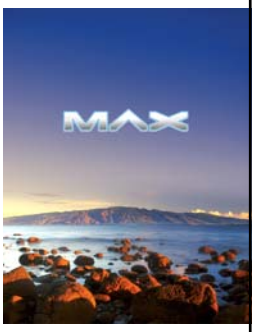
- Role-based
- Declarative Security
- Programmatic Security
- Standards only go so far, for example:
  - the Servlet specification doesn't define logout
- Implementations & extensions vendor specific

FDS Security

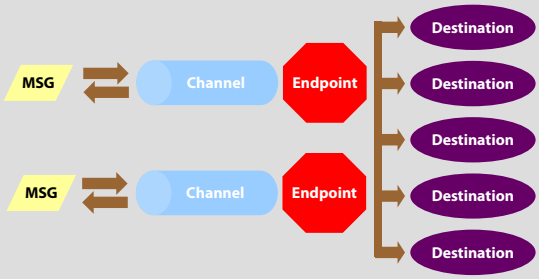
What are destinations, channels and endpoints?

How do you secure an endpoint?

How do you secure a destination?

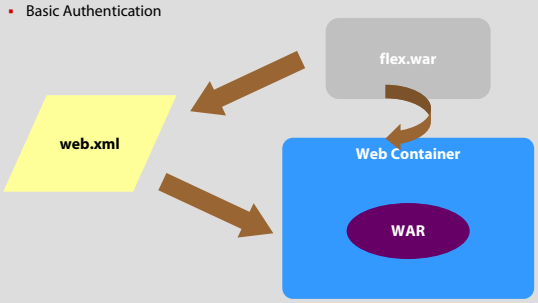


What are destinations, channels and endpoints?



How do you secure an endpoint?

- Basic Authentication



How do you secure a destination?

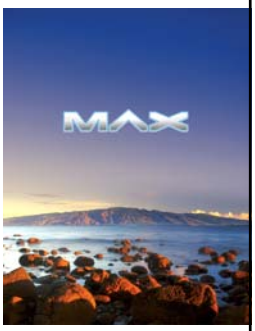
- Basic Authentication
- Custom Authentication

Custom Authentication

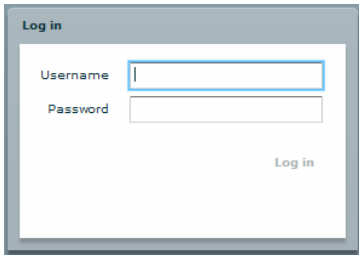
What is custom authentication?

How is the user authenticated?

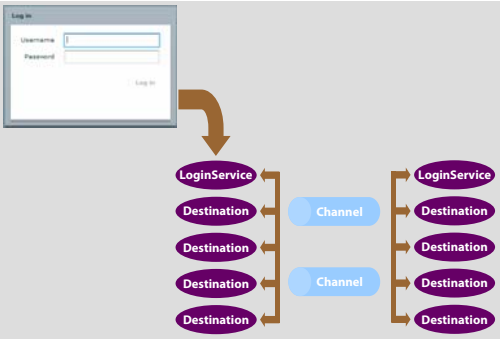
How do you set credentials?



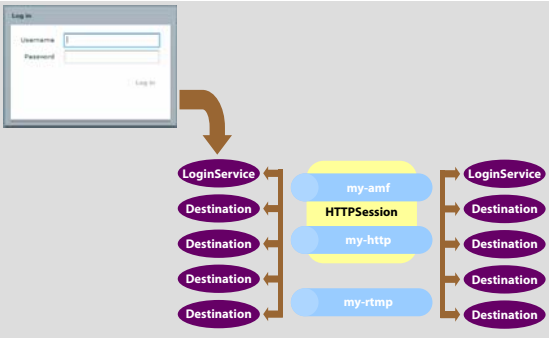
What is custom authentication?



How is the user authenticated?



How does the HTTPSession affect authentication?



How do you set credentials?

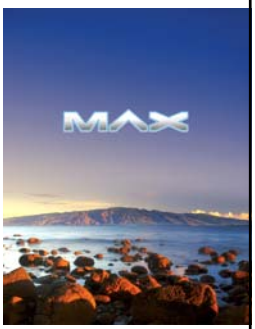
- Accessing secure destinations:
  - AbstractService (RemoteObject, WebService)
  - HTTPService
  - MessageAgent (Consumer, Producer)
  - DataService
- setCredentials(username : String, password : String);
- logout();

What about Cairngrom?

- 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"

Confidentiality

How do you secure the communications link?



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

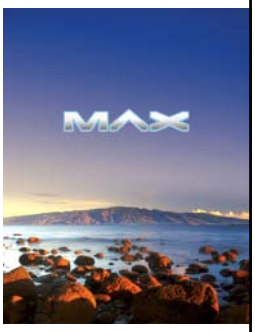
What SSL is not?

- SSL doesn't offer persistent security

"Hello World" ⇨ ZZZZZ CNHBF MTPIH AWNCP SDHGS QEUEE ⇨ "Hello World"

Flash Security

What is relevant to a Flex developer?

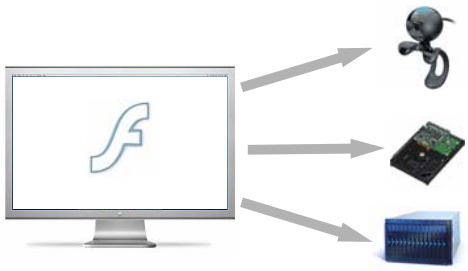


What is relevant to a Flex developer?

- 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

What can the user control?

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



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…

crossdomain.xml ⇦ 

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

What can the developer control?

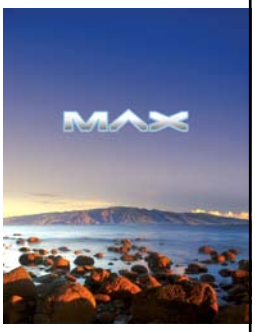
- The Flash Player executes the RIA within its security environment…

Flex Security

What role does Flash play?

What about FDS?

Is there anything else?



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

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

Is there anything else?

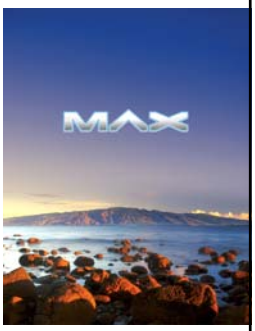
- How do we surface user permissions?

Sample Application

Use Cases

Deployment

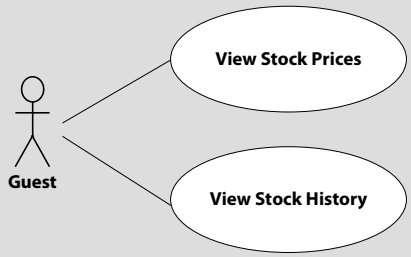
The Code



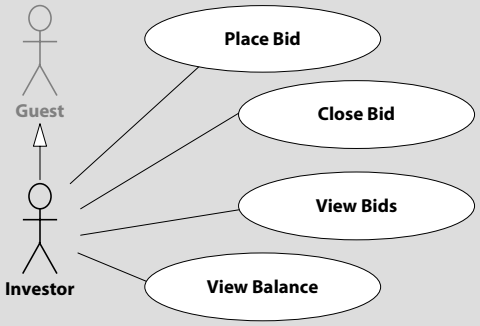
Flex Spread Betting

<<insert screen shot>>

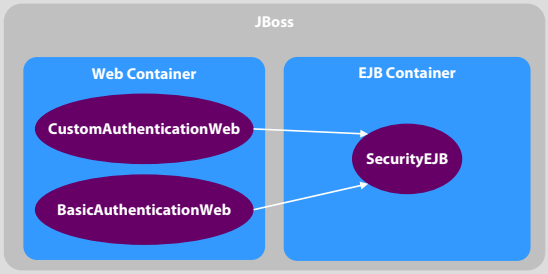
Use Cases – guest



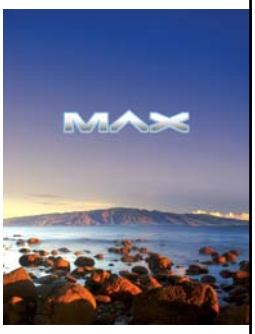
Use Cases – investor



Deployment



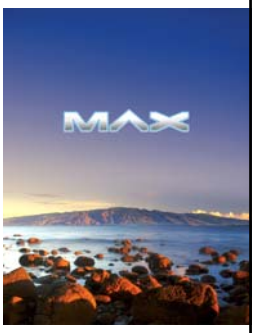
Summary



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

Questions?




Better by Adobe™
2006 Adobe Systems Incorporated. All Rights Reserved.
43
Adobe