



# Testing Flash Applications using WebScarab

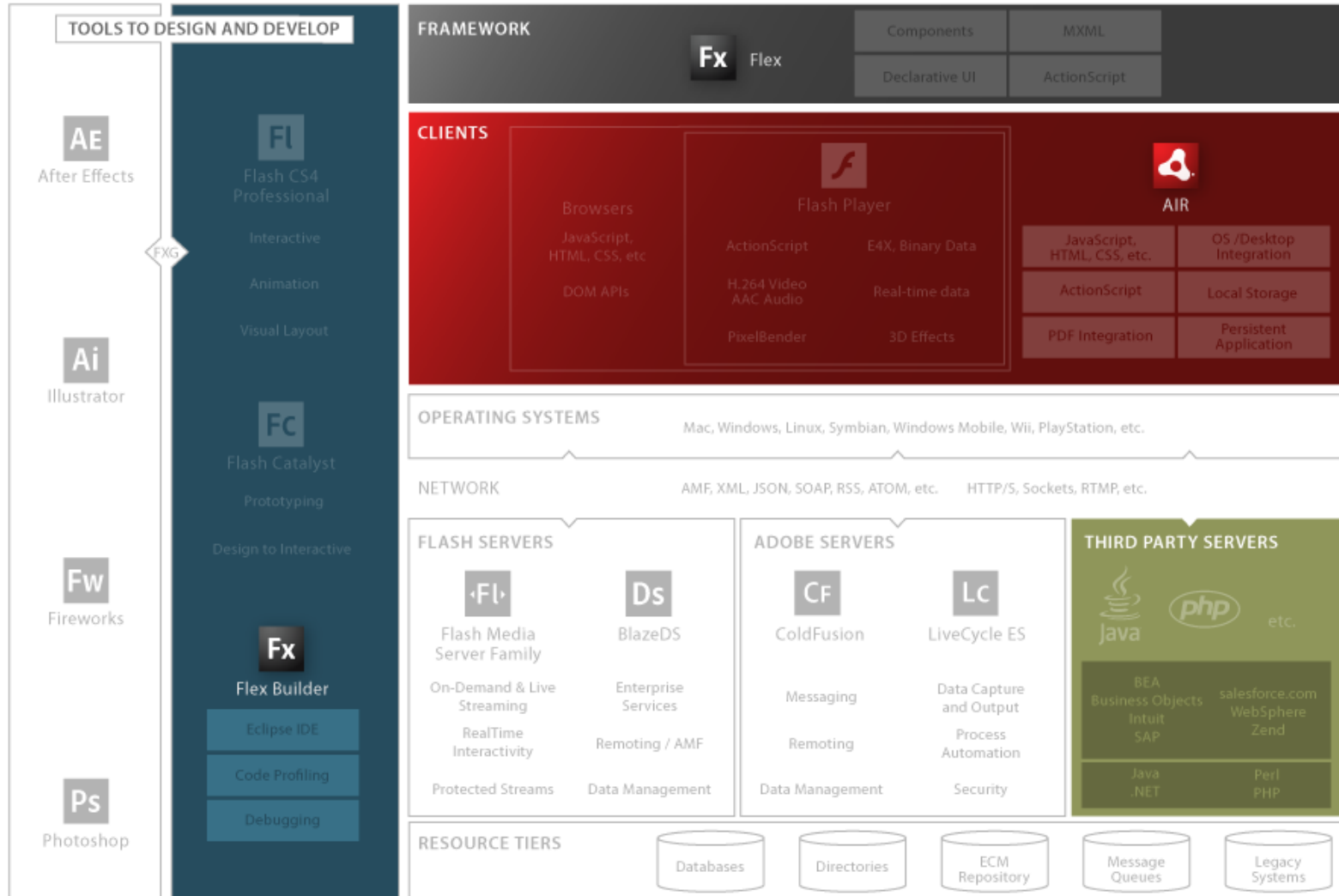
Martin Clausen <mclausen@deloitte.dk>

# Introduction

- Flash
  - Used to create animations, ads, and various Web components, to integrate video into web pages and, more recently, to develop RIA
  - Includes scripting languages - ActionScript 1, 2 & 3
- Flash Player
  - Runs Flash content (SWF file format)
- Flex
  - Framework for developing RIAs that run in Flash Player
  - Design GUI in MXML (XML document) for components, and ActionScript for programming
- Flash application can interact with a web page using JavaScript and vice versa

# Adobe Flash Platform

## Adobe Flash Platform and web technologies



# ActionScript Message Format (AMF)

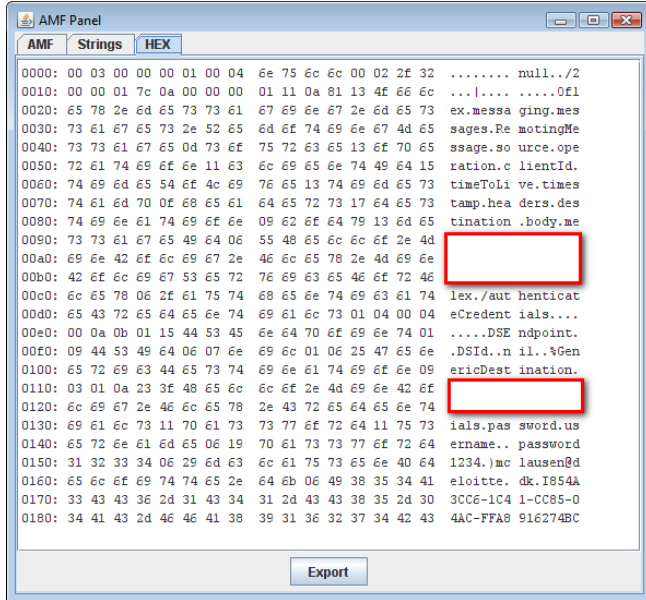
- Mostly used to exchange data between Flash application and server side component
- Asynchronous RPC mechanism, where objects are serialized and deserialized to and from AMF
- AMF is a binary format
  - Like ASN.1 where data is encoded in TLVs
- Two versions: 0 & 3
- Specifications now open

```
$ ./dumpan1 -h sig1.der
<30 45>
0 69: SEQUENCE <
<02 21>
2 33: INTEGER
: 00 C8 7A 3A 87 14 56 DC C6 FF C4 4F F5 CB 8C D1
: F6 BF 47 12 A8 D0 32 E0 25 EE C7 94 CC DC 85 C7
: AD
<02 20>
37 32: INTEGER
: 7C 42 8F 20 B9 4C 6A 11 8C 26 4E 27 AF 63 1E 05
: 53 AB 9F 13 68 E4 BD 19 FC 0E A1 3D 7E 60 12 8D
: >
```

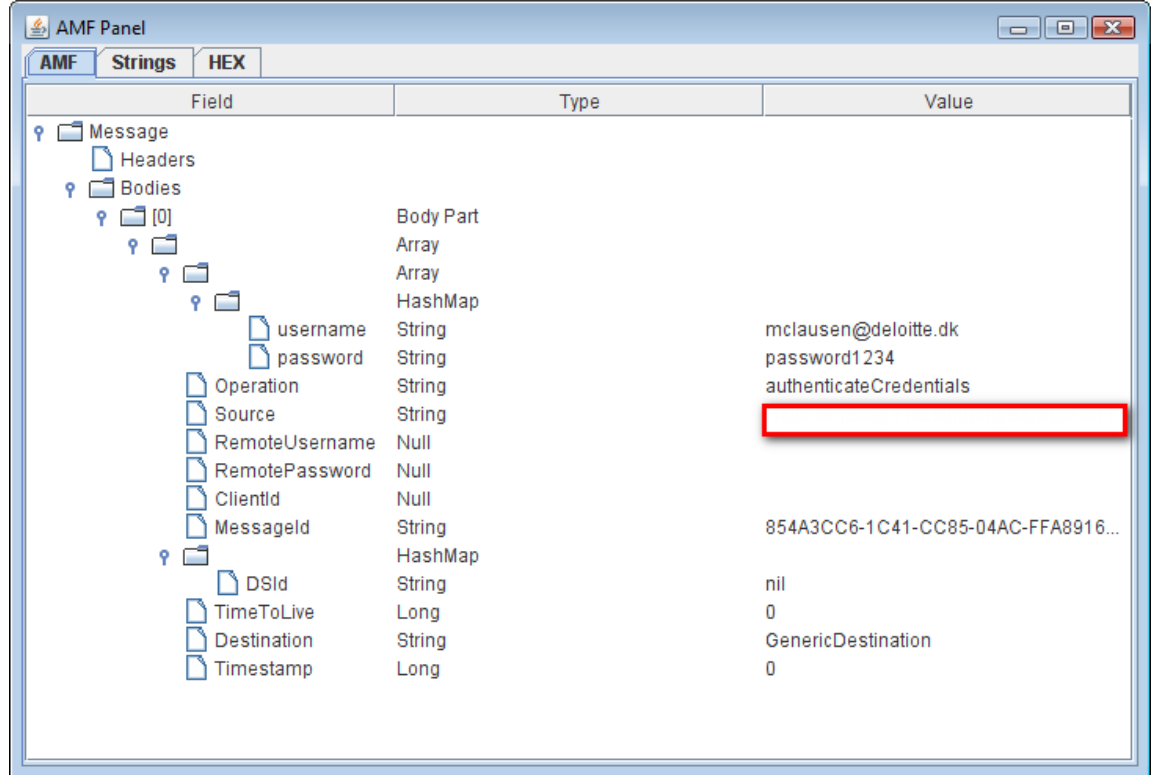
# Remoting envelope

- Preamble containing version: 0 or 3
- Header(s)
  - Name
  - Data: serialized AMF object
- Message(s)
  - Target URI
  - Response URI
  - Data: serialized AMF object

# Remoting example



Raw request



Decoded request

## Text

```

1 00000000null00/2000x
2 000000
3 00Oflex.messaging.messages.RemotingMessageSource0operation0headers0destination body0messageId0clientId0timeToLive0timestamp00/[red box]/authenticateCredentials
4 0000DSEndpoint0SId0nil00%GenericDestination00
5 # [red box] Credentials0username0password0mclausen@deloitte.dk00Test12340IBDE40CA9-EA66-0978-423F-F95FB1485AB300000
    
```

# Techniques

Some support:

- WebScarab
- Charles
- ServiceCapture
- (Burp suite)
- (WireShark)
- No write support!

Write "custom" Flex application:

The screenshot shows a web browser window displaying a Flex application interface. The interface includes a login form with fields for Username, Password, Auth ticket, User ID, Access ticket, Validate, Logoff, Echo in, Echo out, Current user, and Device UID. The Current user section displays a table of user information.

Field	Value
Username	mclausen@deloitte.dk
E-mail	mclausen@deloitte.dk
User ID	3a5a2895-a571-448b
Last signon	Wed Dec 3 16:48:09
Cellphone	30934215
Password	Test1234
Is registered	true

# WebScarab AMF extension

- WebScarab supports a plugin “infrastructure”
- Our plugin:
  - Replaces the existing (reads AMF 0)
  - Supports AMF 0 & 3
  - Supports read / write
  - Still in development



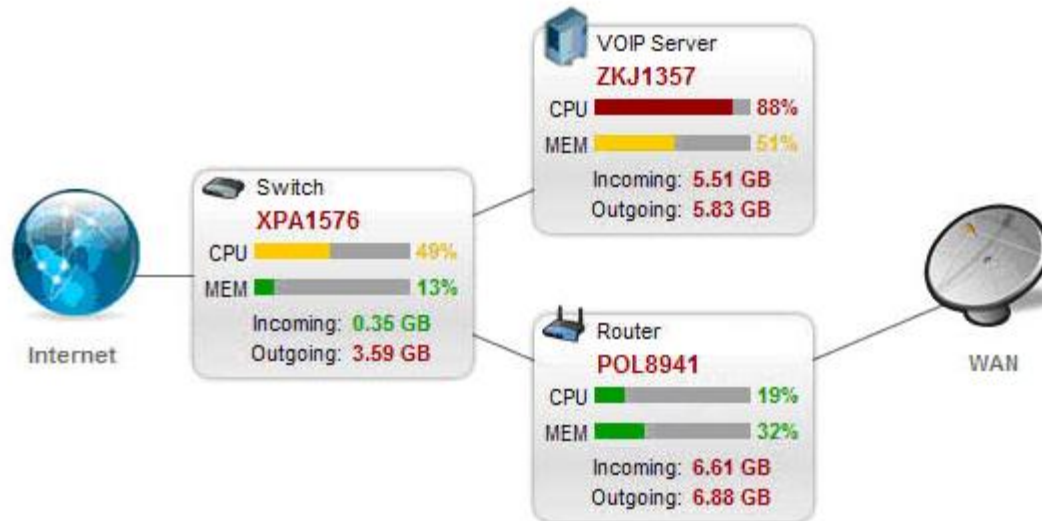
# WebScarab AMF extension – ctd.

The screenshot displays two captured AMF messages in WebScarab. The top message is a POST request to `http://examples.adobe.com:80/flex3app/netmondata/messagebroker/amf` with a status of 200 OK. The AMF data shows a `Message` object with a `BodyPart` array containing a `String` value of `getDeviceDetail HELLO WORLD`.

The bottom message is a response with a status of 200 OK. The AMF data shows a `Message` object with a `BodyPart` array containing an `AcknowledgeMessageExt` object. The object contains the following fields:

Field	Type	Value
SmallMessage	AcknowledgeMessageExt	Flex Message (flex.messaging.messages.AcknowledgeMessageExt) clientId = n...
CorrelationId	String	5485852F-5C61-8AAA-4FC9-F9775F3EE734
incoming	Double	7.25508975982666
location	String	San Jose, CA
iconUrl	Null	

# Demo



# More information

- Testing Flash Applications (Stefano Di Paola / OWASP):  
[http://www.wisec.it/en/Docs/flash\\_App\\_testing\\_Owasp07.pdf](http://www.wisec.it/en/Docs/flash_App_testing_Owasp07.pdf)
- Adobe Flash Player 9 Security:  
[http://www.adobe.com/devnet/flashplayer/articles/flash\\_player\\_9\\_security.pdf](http://www.adobe.com/devnet/flashplayer/articles/flash_player_9_security.pdf)
- AMF 0 Specification:  
[http://download.macromedia.com/pub/labs/amf/amf0\\_spec\\_121207.pdf](http://download.macromedia.com/pub/labs/amf/amf0_spec_121207.pdf)
- AMF 3 Specification:  
[http://download.macromedia.com/pub/labs/amf/amf3\\_spec\\_121207.pdf](http://download.macromedia.com/pub/labs/amf/amf3_spec_121207.pdf)
- OWASP / WebScarab:  
<http://www.owasp.org>
- Open Source Flash:  
<http://osflash.org>