分析Adobe Flash

构建Flash平台的模糊测试工具

基于文件格式的Adobe Flash漏洞挖掘框架

介绍

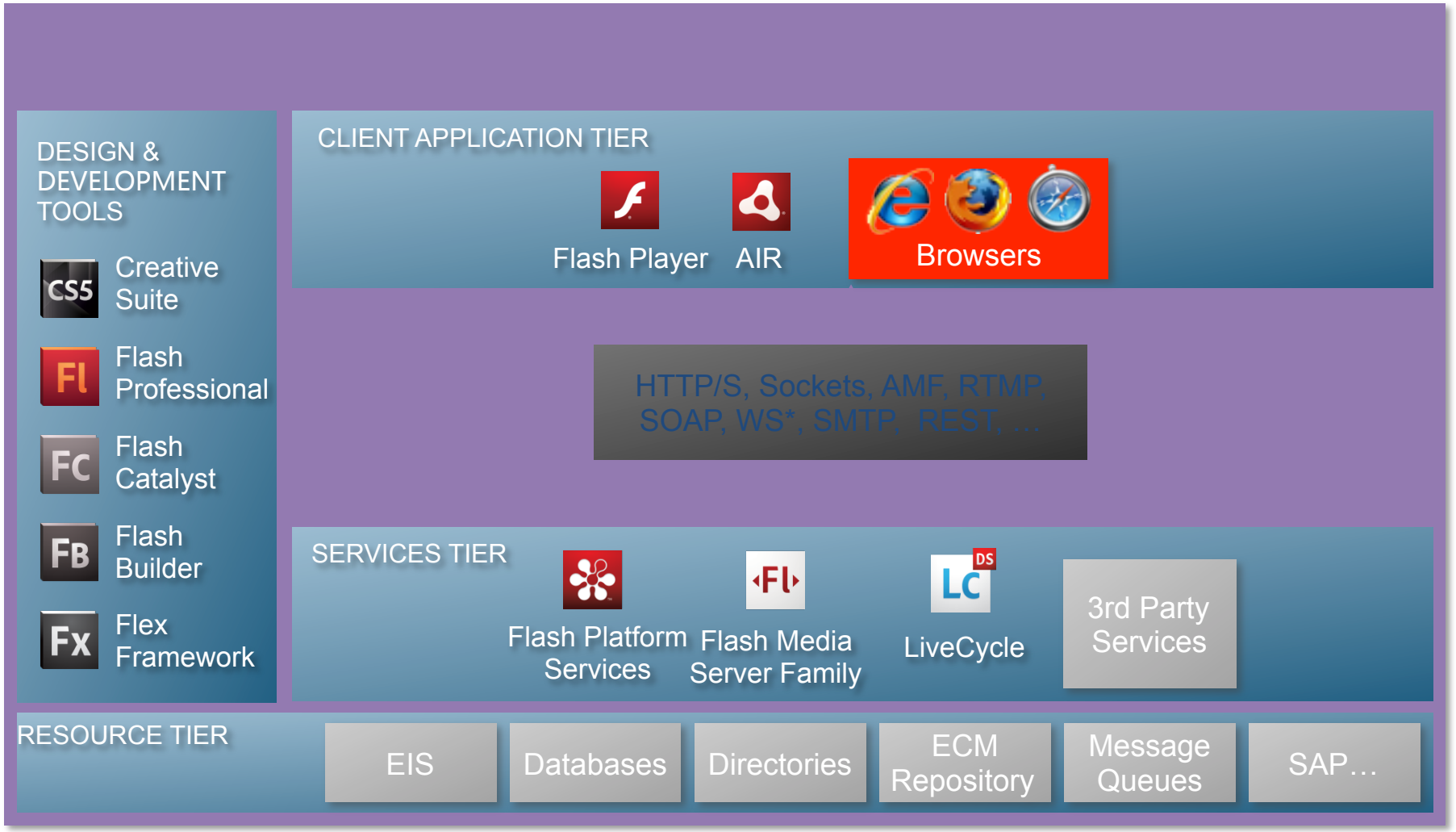
- Nick
  - 宋国徽
  - cis7all@gmail.com
- 研究方向
  - 应用安全
  - 逆向工程
  - 漏洞挖掘
  - 渗透测试
  - 情报分析
  - 产业研究

- 主要经历
  - 2012年至今，上海八六三信息安全产业基地
  - 2011年至今，OWASP中国区，上海地区负责人
  - 2011年至今，江西高校网络安全知识及软件设计大赛—专家委员组成员
  - 2009年至今，上海市信息安全技能竞赛—专家委员组成员
  - 2008年至今，创办ISF安全会议，ISF2008/ISF2009/ISF2010/ISF2011/ISF2012
  - 2007年至今，IDF Labs的联合创始人
  - 2006年至今，在线安全团队CISRG的发起人
  - ……

为什么是Adobe Flash?

- Flash = %99 = 富互联网应用
- 客户端攻击
- Flash是一个平台，并不仅仅是浏览器插件

Adobe Flash架构



介绍

面向Flash文件格式模糊测试

面向Flex框架的模糊测试

总结

Flash文件格式模糊测试工具

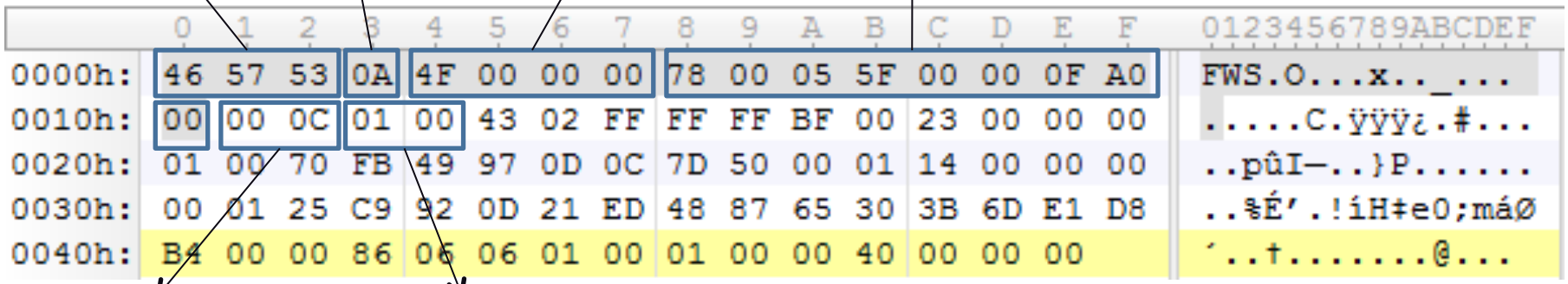
- SWF文件格式
- 解压SWF文件
- 构建模糊测试工具
- 演示

SWF文件格式

- 解析SWF文件头

RECT
Nbits UB[5]
Xmin SB[Nbits]
Xmax SB[Nbits]
Ymin SB[Nbits]
Ymax SB[Nbits]

签名　版本　文件大小　边框大小



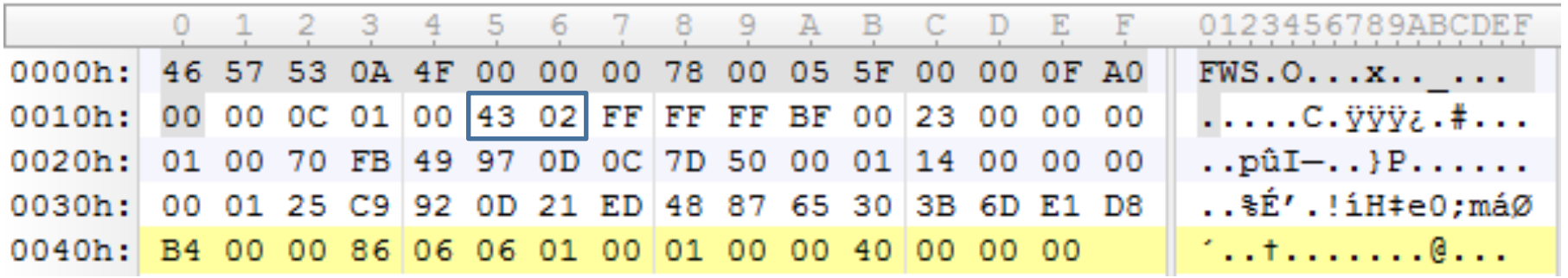
每帧速率　帧数量

0111 1000 0000 0000 0000 0101 0101 1111 0000
0000 0000 0000 0000 1111 1010 0000 0000

01111 = 15

SWF文件格式

- 解析SWF 标签
  - RecordHeader(短类型标签)
    - TagCodeAndLength (UI16)
      - 标签标识符 – TagCode (10 bits)
      - 标签数据长度 – TagLength (6 bits)
    - 标签数据
      - 数据结构
    - 例如: SetBackgroundColor/ShowFrame/…

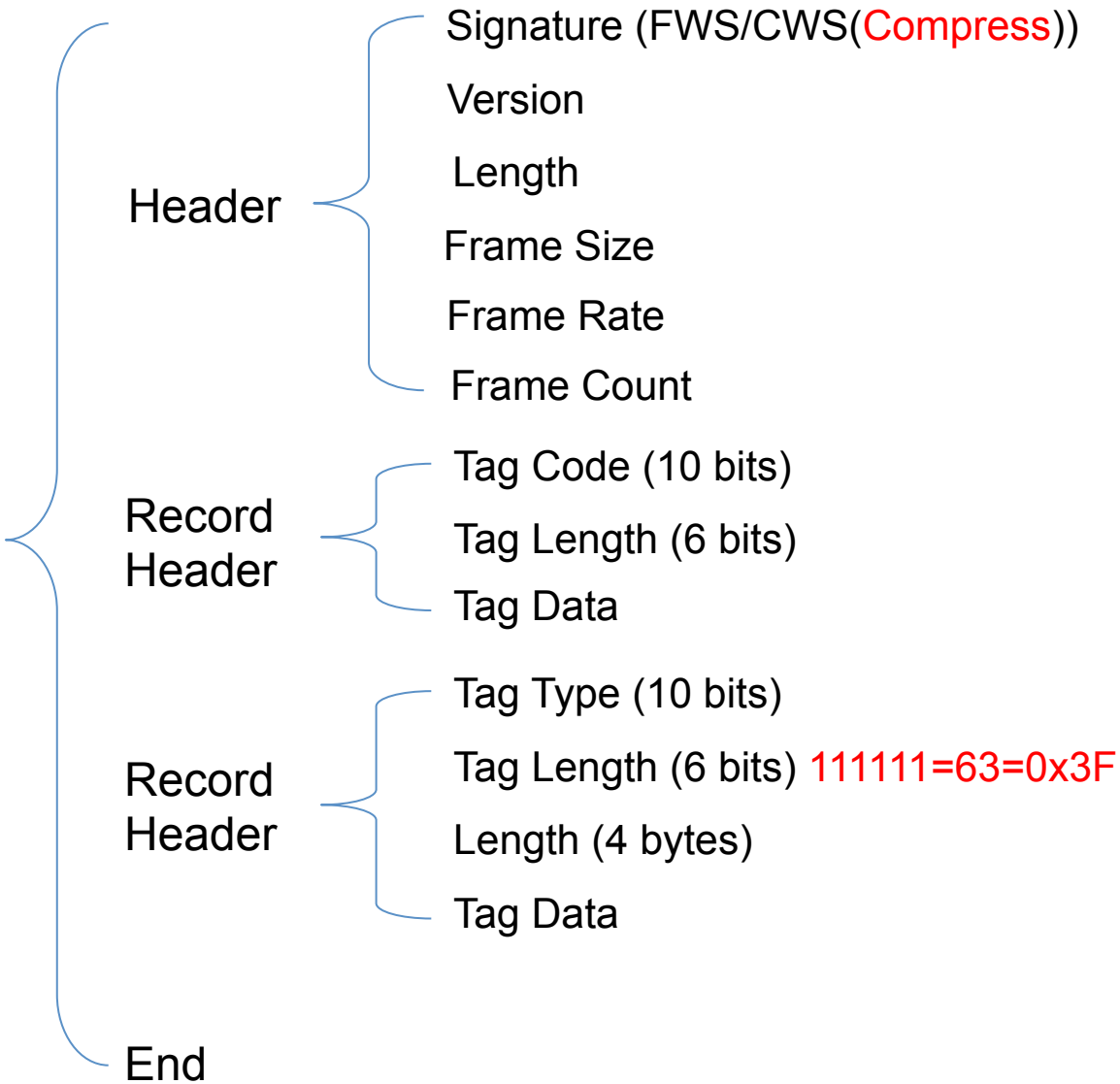


	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	46	57	53	0A	4F	00	00	00	78	00	05	5F	00	00	0F	A0	FWS.O...x.._...
0010h:	00	00	0C	01	00	43	02	FF	FF	FF	BF	00	23	00	00	00	.....C.ÿÿÿ¿.#...
0020h:	01	00	70	FB	49	97	0D	0C	7D	50	00	01	14	00	00	00	..pûI—..}P.....
0030h:	00	01	25	C9	92	0D	21	ED	48	87	65	30	3B	6D	E1	D8	..%É'.!íH‡e0;máØ
0040h:	B4	00	00	86	06	06	01	00	01	00	00	40	00	00	00		´..†.......@...

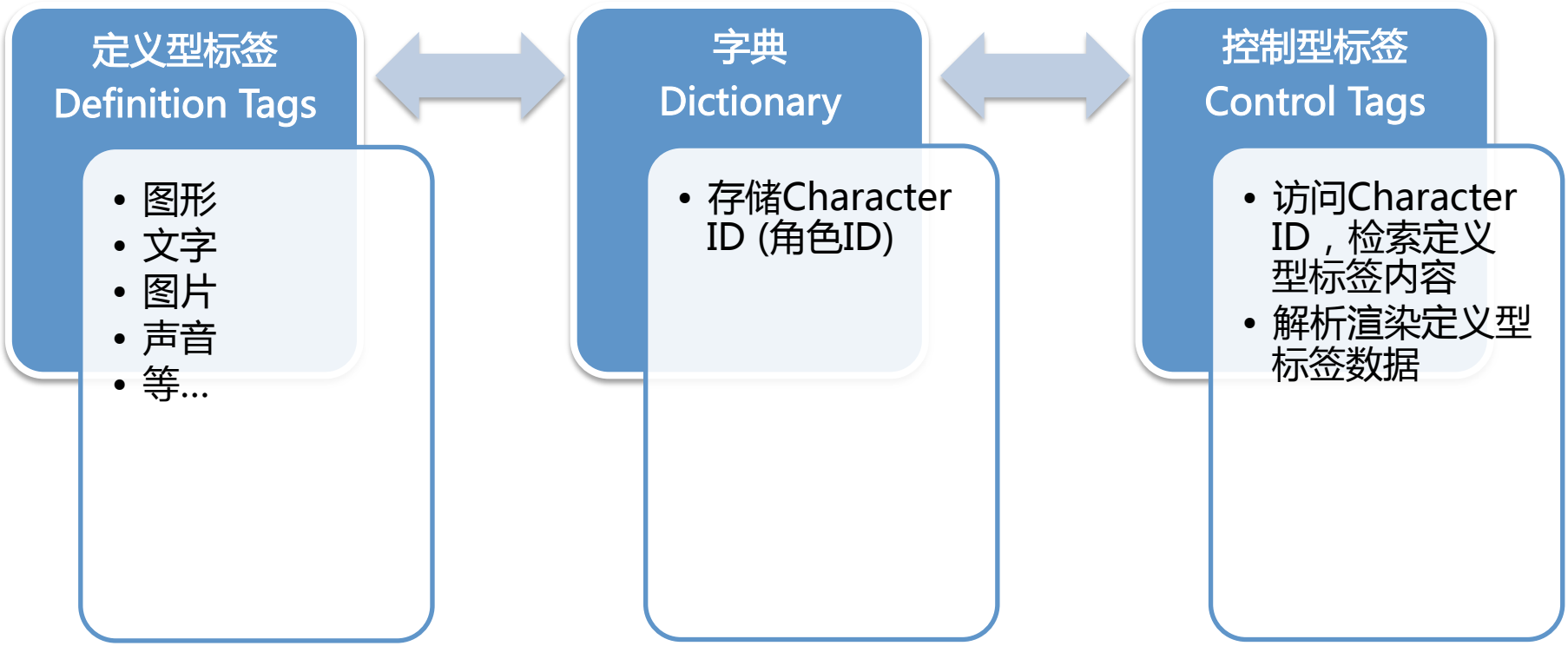
SWF文件格式

- 解析SWF 标签
  - RecordHeader(长类型标签)
    - TagCodeAndLength (UI16)
      - 标签标识符 - TagCode(10 bits)
      - 标签数据长度 - TagLength(6 bits) (111111 = 63 = 0x3F)
    - 数据长度 - Length(UI32)
      - 4 bytes
    - 标签数据
      - 数据结构
    - 例如: MetaData/DoABC/...

SWF文件格式


Header
Signature (FWS/CWS(Compress))
Version
Length
Frame Size
Frame Rate
Frame Count
Record Header
Tag Code (10 bits)
Tag Length (6 bits)
Tag Data
Record Header
Tag Type (10 bits)
Tag Length (6 bits) 111111=63=0x3F
Length (4 bytes)
Tag Data
End

SWF文件格式


定义型标签
Definition Tags
• 图形
• 文字
• 图片
• 声音
• 等…
字典
Dictionary
• 存储Character ID (角色ID)
控制型标签
Control Tags
• 访问Character ID，检索定义型标签内容
• 解析渲染定义型标签数据

解压SWF文件

- CWS格式
  - zlib (CWS_2_FWS)

```
import sys, os
import zlib, struct

fp = open('*.swf', 'rb')
flag = ''.join(struct.unpack('<3C', fp.read(3)))
header['compress'] = flag.startswith('C')
header['version'] = struct.unpack('<B', fp.read(1))[0]
header['size'] = struct.unpack('<I', fp.read(4))[0]
if header['compress']:
    compress_data = fp.read(header['size'])
    uncompress_data = zlib.decompress(compress_data)
    ……
fp.write(uncompress_data)
……
```

构建模糊测试工具

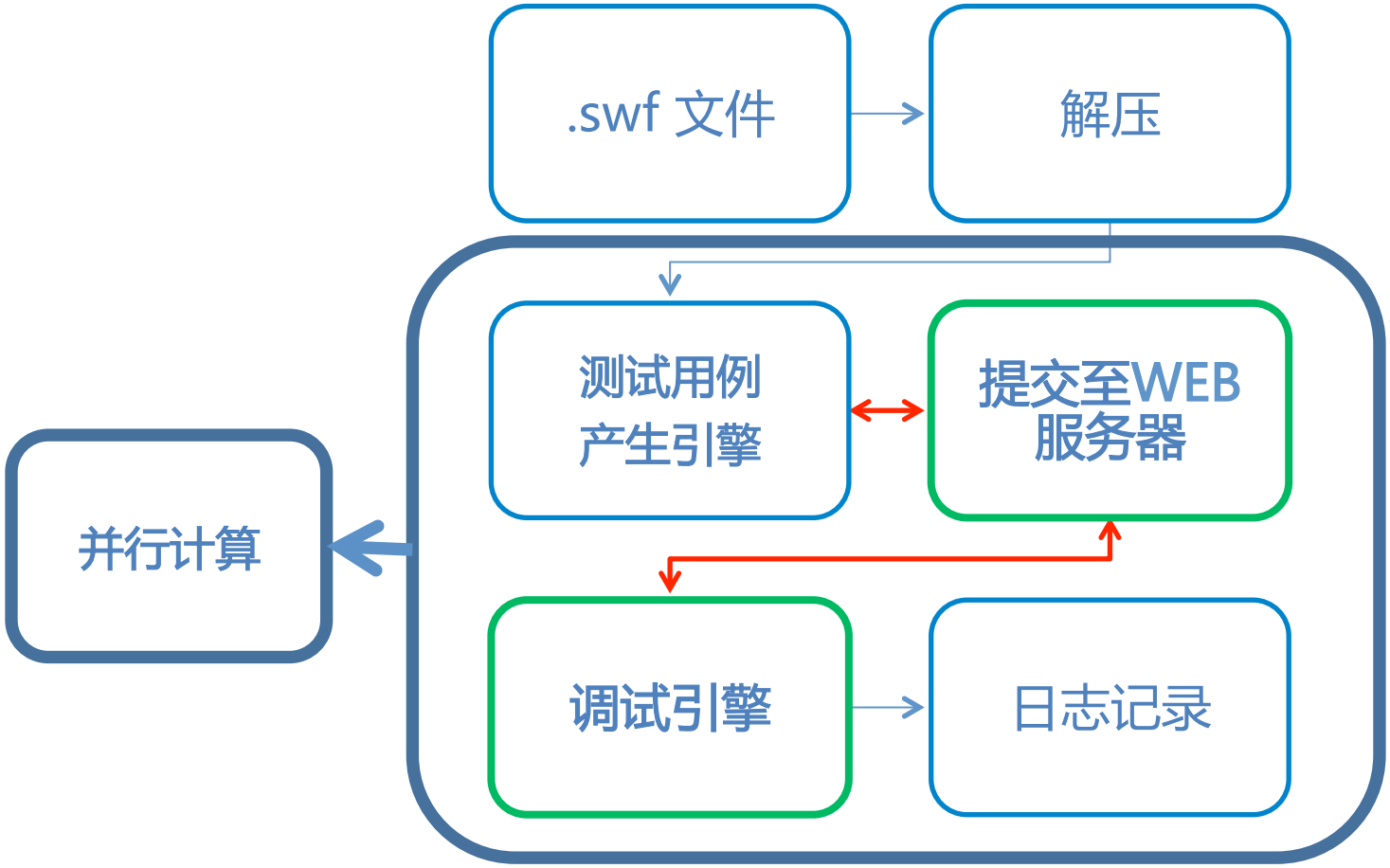
- 模糊测试工具
  - 测试用例产生引擎
    - 标签数据
      - 简单类型 例如: SetBackgroundColor
      - 数据结构 例如: DefineBitsJPEG2
      - 复杂类型
        - » Def-Tag + Def-Tag = Def-Tag(new)
    - 标签长度
      - TagLength
      - Length

构建模糊测试工具

- 模糊测试工具
  - 调试器
    - Pydbg（python模块）
      - windbg
  - 日志记录
    - 崩溃信息

构建模糊测试工具

- 框架



演示

Flex框架模糊测试工具

- ActionScript和AVM2虚拟机介绍
- Flex框架介绍
- AVM虚拟机与ABC文件
- ActionScript语法分析器
- 构建模糊测试工具
- 演示

AS3 & AVM2

- ActionScript3
  - Flash9/10
  - AVM2
    - 项目代号：Tamarin
    - 开源项目(Mozilla)

AS3 & AVM2

- AVM2
  - Tamarin
    - ABC文件 & ABCASM & DoABC标签
    - **关爱动物，保护我们的家园!**

Flex框架介绍

- Adobe Flex 框架
  - 产品部署
    - Flash Pro
    - Flash Builder(aka: Flex Builder)
  - 开源，包括：
    - asc
    - mxmlc
    - compc
    - SDK 中的所有API
    - 等等……

svn co http://opensource.adobe.com/svn/opensource/flex/sdk/trunk/ flex_sdk_svn

AVM虚拟机与ABC文件

- 编译器
  - Tamarin
    - avmshell -> Tamarin
    - avmplus -> Flex Framework

```
7all@CISRG:as3_example$ls
avmplus.exe  avmshell.exe  hello.as

7all@CISRG:as3_example$cat hello.as
print ("hello world");
7all@CISRG:as3_example$./avmshell.exe hello.as
hello world

7all@CISRG:as3_example$./avmplus.exe hello.as
VerifyError: Error #1042

7all@CISRG:as3_example$
```

AVM虚拟机与ABC文件

- 编译器 – asc.jar / asc.exe

svn co http://opensource.adobe.com/svn/opensource/flex/sdk/trunk/modules/asc asc

```
7all@CISRG:as3_example$ls
avmplus.exe  avmshell.exe  hello.as

7all@CISRG:as3_example$asc hello.as

hello.abc, 85 bytes written

7all@CISRG:as3_example$ls
avmplus.exe  avmshell.exe  hello.abc  hello.as

7all@CISRG:as3_example$./avmshell.exe hello.abc
hello world

7all@CISRG:as3_example$./avmplus.exe hello.abc
hello world

7all@CISRG:as3_example$
```

AVM虚拟机与ABC文件

```
package
{
    class cls
    {
        function foo()
        {
            var str:String = "Hello ISF2010!";
            print (str);
        }
    }
    var obj:cls = new cls();
    obj.foo();
}
```

AVM虚拟机与ABC文件

```
7all@CISRG:as3_example$asc.exe as_hello.as

[Compiler] Error #1017: The definition of base class Object was not found.
   as_hello.as, Ln 1, Col 1:
   package
   ^

1 error found

7all@CISRG:as3_example$asc.exe -import $BUILTINABC as_hello.as

as_hello.abc, 255 bytes written

7all@CISRG:as3_example$./avmshell.exe as_hello.abc
Hello ISF2010!

7all@CISRG:as3_example$./avmplus.exe as_hello.abc
Hello ISF2010!
```

AVM虚拟机与ABC文件

- ABC文件的基础元数据

builtin.abc

```
include "Object.as"
include "Class.as"
include "Function.as"
include "Namespace.as"
include "Boolean.as"
include "Number.as"
include "String.as"
include "Array.as"
include "actionscript.lang.as"
include "Vector.as"
include "DescribeType.as"
```

shell_toplevel.abc

include meta class

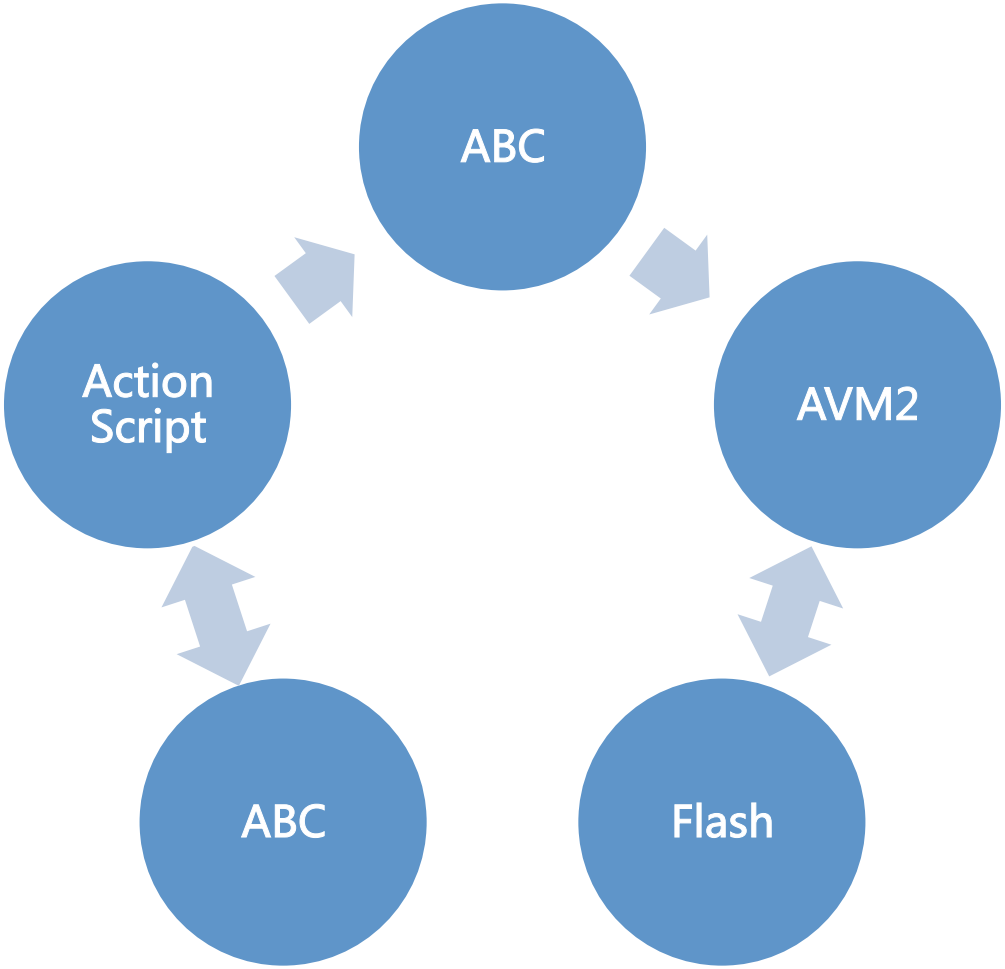
playerglobal.abc

meta package and class for flash

AVM虚拟机与ABC文件

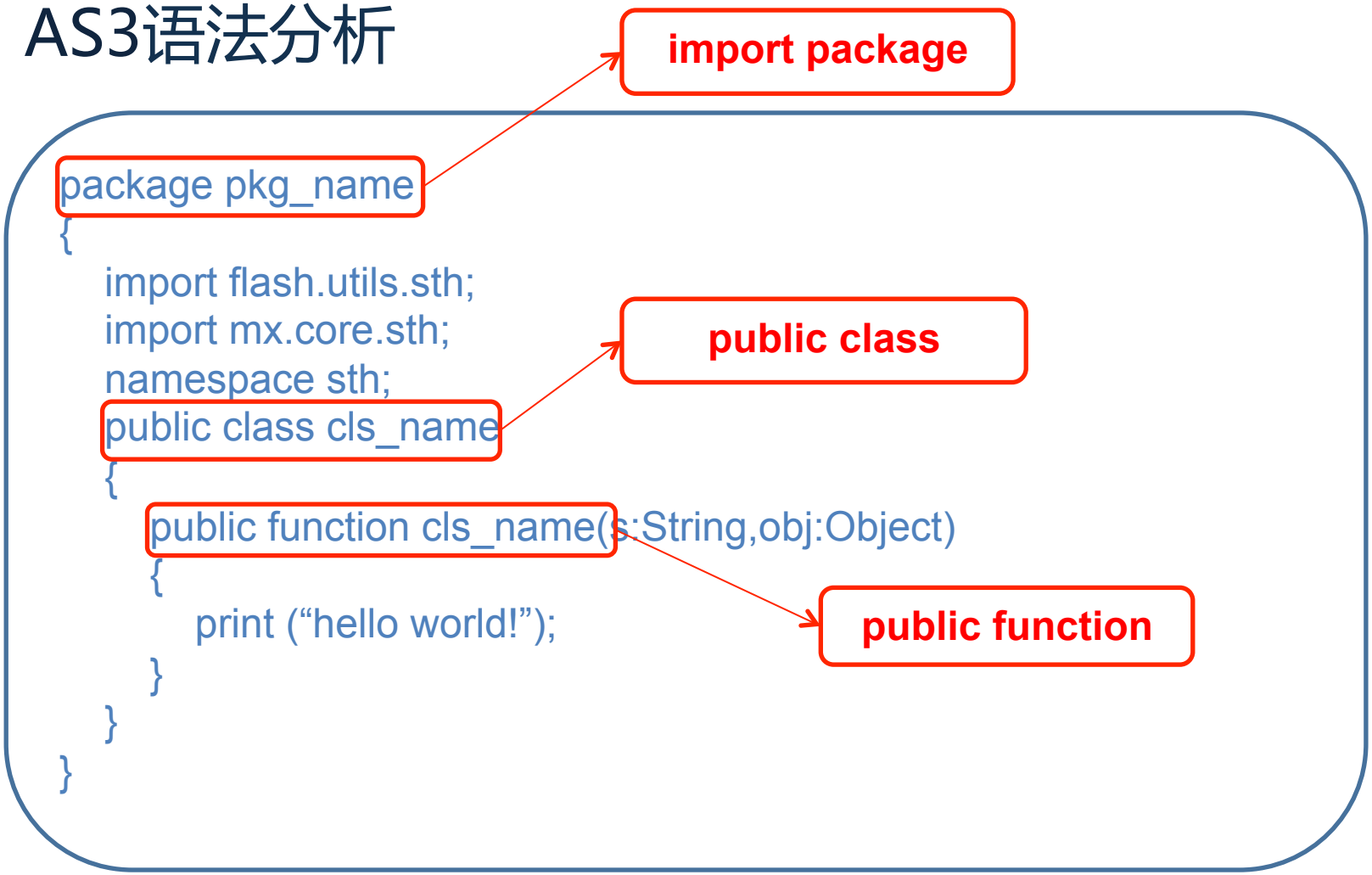
- AVM2机制与原理
  - AVM2的基础是ABC文件
  - ActionScript编译时所需要的基础数据结构均来自于ABC文件
  - Native API和Public API都来自于ABC文件
  - 对ABC文件进行模糊测试
    - 构建ActionScript模糊测试器

AVM虚拟机与ABC文件



ActionScript语法分析器

- AS3语法分析



ActionScript语法分析器

- AS3语法分析
  - PLY -> Python Lex-YACC
    - BNF
    - AST
      - package
      - public class
      - public function(args...)

```
[AS3 Grammar]
Class:          ButtonBar
Function:       ButtonBar()
Function:       borderMetrics()
Function:       direction(value:String)
Function:       moduleFactory(moduleFactory:IFlexModuleFactory)
Function:       viewMetrics()
Function:       styleChanged(styleProp:String)
Function:       drawFocus(isFocused:Boolean)
```

构建模糊测试工具

- 模板系统
  - Cheetah
    - Python下的模板系统

```
package {
    import $pkg['package'].*;
    public class cls
    {
        #for $cls in $pkg
        #if $cls is not 'package‘
        #set $obj = 'obj‘
        #set $fck = '()‘
        var $obj:$cls = new $cls$fck
        #for $foo in $pkg[$cls]
        $obj.$foo
        #end for
        #end if
        #end for
    }
}
```

构建模糊测试工具

普通模板

```
var obj = new Object();
obj.foo1(-1);
obj.foo2(“AAA…AAA”);
obj.foo2(“../../../…../../../”);
obj.foo2(“%n%n%n…%n%n%n”);
…
obj.foox([1,[2,[3],4],5…,x]);
…
obj.foon(“<xml>…</xml>”);
```

特殊模板（UAF）

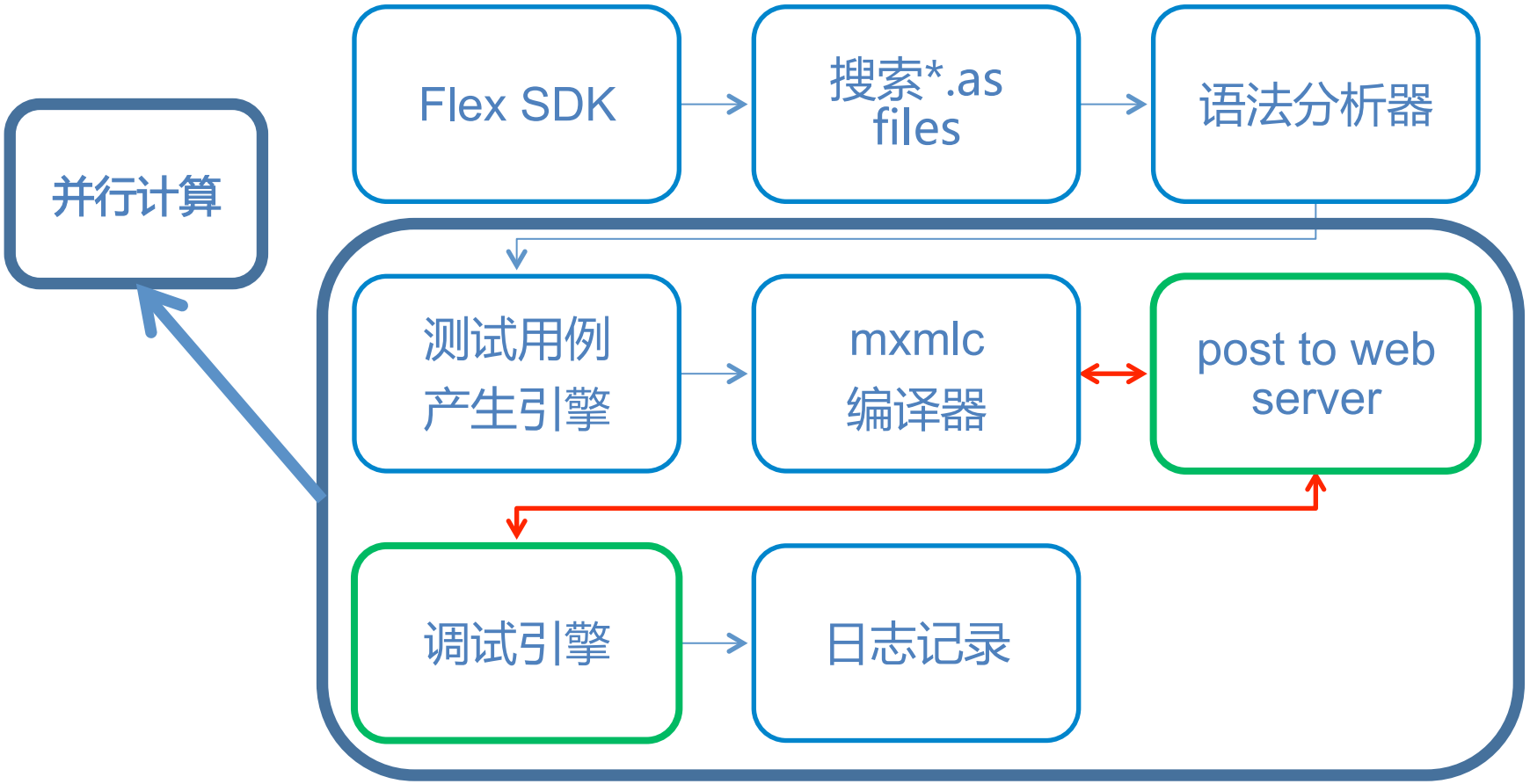
```
var obj = new Object();
obj.call()
var after = obj;
after.call()
delete(obj)
after.call()
…
after = copy(obj)
delete(obj)
after.call()
```

构建模糊测试工具

- Flex框架下编译器
  - mxmlc
    - 编译器

构建模糊测试工具

- 框架


并行计算
Flex SDK
搜索*.as files
语法分析器
测试用例产生引擎
mxmlc编译器
post to web server
调试引擎
日志记录

演示

总结

- 漏洞挖掘 vs 运气
  - 如何提高漏洞挖掘能力?
    - 基础知识的扎实程度
    - 逆向工程的能力
    - 分析漏洞和编写漏洞利用代码的能力
    - 漏洞挖掘的实践能力
  - **没有运气!!!**
  - **1%(运气) + 99%(汗水)**

None

Question?