Short Attention Span Security

Ben Kurtz

awgh at awgh.org

Wait... What?

- 5-7 Turbo Talks (time permitting):
  - Script Injection in Flex
  - Rant in EFI
  - Static Analysis with Dehydra
  - ITX and Wifi Hacking
  - Some Surprises...

Weaponizing Mailinator

- I’ll give you a toy to play with while I get along with the rest of my talk.

What’s Mailinator?

- Website that offers anonymous email service
- Any email sent to any address of any Mailinator domain is publicly viewable via mailinator.com
- It seems people mostly use this for porn, torrents, or dating sites...

Mailinator-nator

- Script A does the following:
  - Brute forces 'Forgot Password' fields that only require email addresses on a list of sites, using a userlist.
  - For each username, tries each of the Mailinator domain aliases.

Mailinator-nator

- Script B does the following:
  - Reads a userlist from a file
  - For each word, connects to Mailinator and logs all emails to that user which contain the word ‘password’
  - Fun as a cron job with a good wordlist...

Inspiration

- “My name is Sarah Palin and I’ve forgot my password, gosh darn it!”
- The ‘Forgot Password’ page exists solely to allow unauthorized users to bypass the usual means of authorization
- These pages usually don’t check for brute forcing, among other problems

WTF, really?

- This doesn’t appear to violate Mailinator’s terms of service...
- They don’t appear to HAVE terms of service!
- IANAL: If you actually log in using a ‘remembered’ password, this is probably illegal.

These scripts are available at:
http://www.awgh.org/files/natornator.tgz

All code and information from this talk is available at:
awgh.org

Smooth Transition (fnord!)

Tell me a story...

Once upon a time,
there was a network administrator...

No-one expects the BIOS Rootkit!

Unexpected?

- Most people don't think of BIOS/PCI Option ROMs as attack surface, but HW attack vectors made the news in 2008:
  - Did you buy a Catalyst on eBay?
  - USB Picture Frame phones home

Delivering a BIOS Rootkit

- Can be flashed to BIOS as an additional module (some secure chipsets require signing)
- Can be flashed to PCI Option ROMs
- Both of these methods can be done with root/Administrator privs (iopl 3)
- Some devices can be reflashed via PXE

Find a way to hang on...

- Most BIOS code runs once, at boot
- The second problem for a BIOS rk is finding a way to run rk code when the OS is in flight
- Definitive works:
  - In ACPI ML - John Heasman 2006
  - With SMM - Black Hat 08 (no code)
  - SMM - Go ask Peter Stuge of coreboot!

Things Are Hard

- System Management Mode lets you trap IO port reads, so you could just trap port 60 for a PS2 keylogger and trigger BIOS code
- Getting USB is deep magic. If you have a way to do this, raise your hand please.
- Legacy BIOS is all 16-bit. Nuff said.
- ACPI relies on the OS using ACPI (but most do)

Things Get Easier

- EFI was developed by Intel to make BIOS development easier (really just to get away from 16-bit mode) but not much security
- The EFI Dev Kit (EDK) from tianocore.org provides pre-made C libraries for:
    - TCP/IP, PXE, and other network functions
    - Filesystem drivers

New Vectors

- Some Apple end-users already familiar with downloading and installing EFI modules (like rEFIt)
- EFI would make it really easy to get rw access to the filesystem from BIOS (not as sexy as SMM), for example:
  - BIOS writes a rootkit to disk
  - BIOS emails me your shadow file

EFI 2009

- EFI has slowly been replacing old BIOS, but the tipping point will be this year
- In 2009, Intel, AMD, and Apple will all be shipping EFI compatible boards by default (Intel and Apple are already there for the most part)

TPM and Option ROMs

- Common misconception that TPMs fix Option ROMs (including in 06 papers)
- This could be implemented, but new sigs would need to be generated every time a PCI card was added
- PCI Option ROMs just run w./ Ring 0 in EFI too... This time in EBC

Hardware Anti-Virus?

- A Web-of-Trust system similar to SSL certificate signing could be created to provide a way for BIOS to verify the validity of Option ROMs
- A list of Option ROMs would have to be white-listed
- Also, BIOS would need a net connection when a new device was detected

And now...

Random XSS

- The Microsoft version of libxml treats a paired start and end tag as a single object. (Why aren't my end tags empty?)
- It also allows end tags to have attributes.
- The last version of the MS anti-XSS ISAPI filter triggered only on a < followed by any letter.

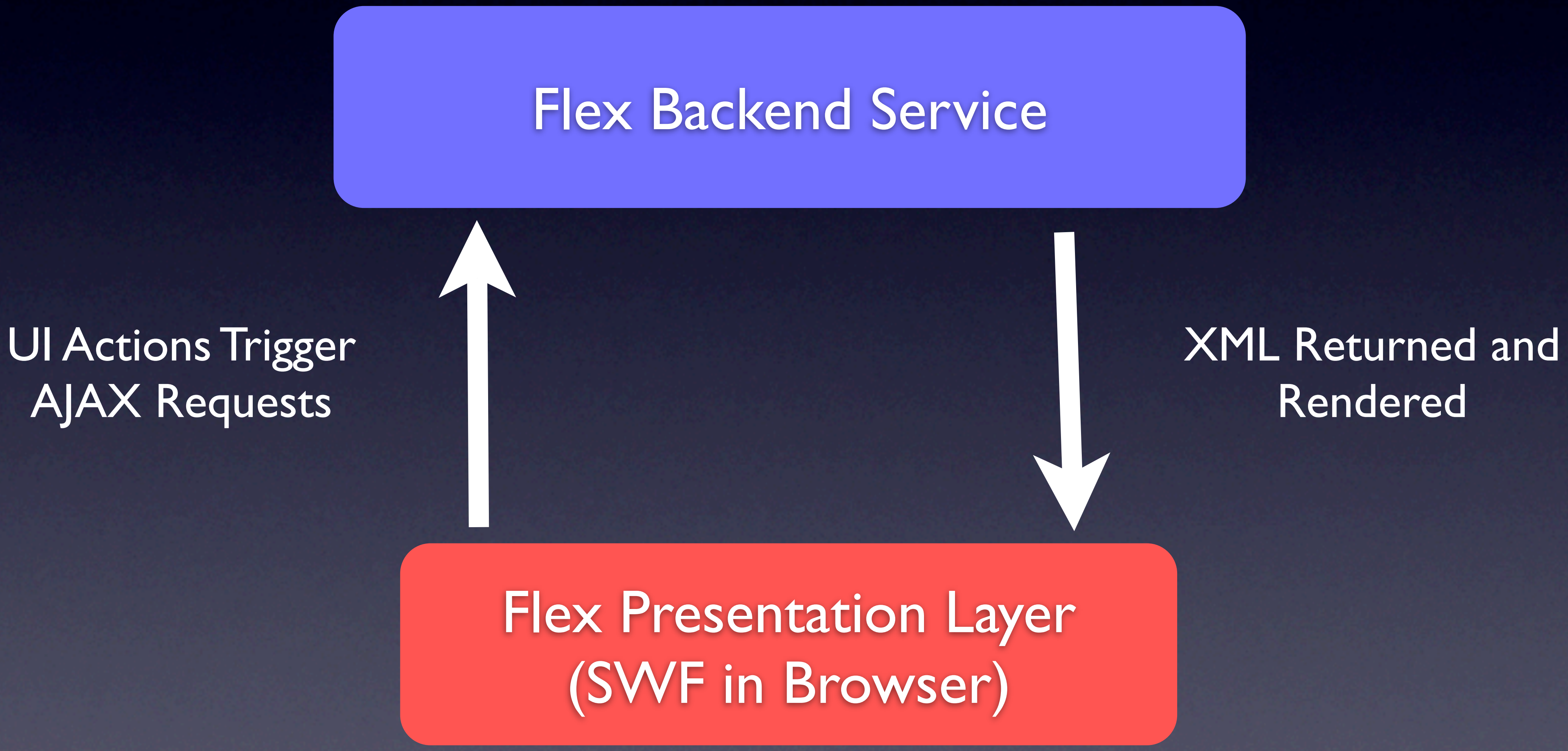
```
</a style=”background:expression(alert(23))” >
```

This is my favorite

Script Injection in Flex

- Macromedia Flex is a Flash-based web platform that is becoming very popular
- Flex offers developers a set of UI widgets that already sanitize and filter all inputs
- Finding a simple XSS or other injection in the usual way leads to disappointment

Script Injection in Flex (cont.)



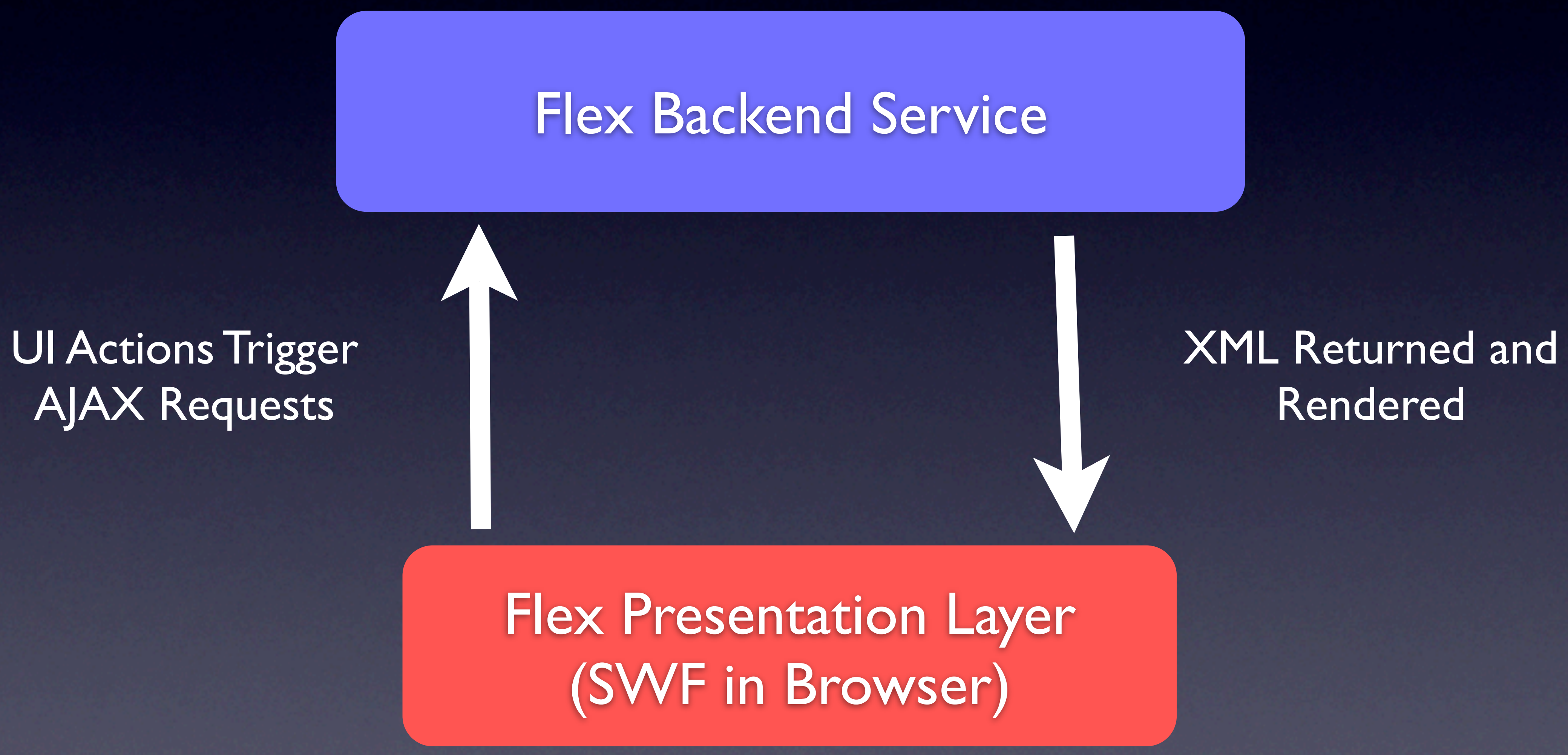
Flex Backend Service

UI Actions Trigger AJAX Requests

XML Returned and Rendered

Flex Presentation Layer (SWF in Browser)

Script Injection in Flex (cont.)



Flex Backend Service

UI Actions Trigger
AJAX Requests

XML Returned and
Rendered

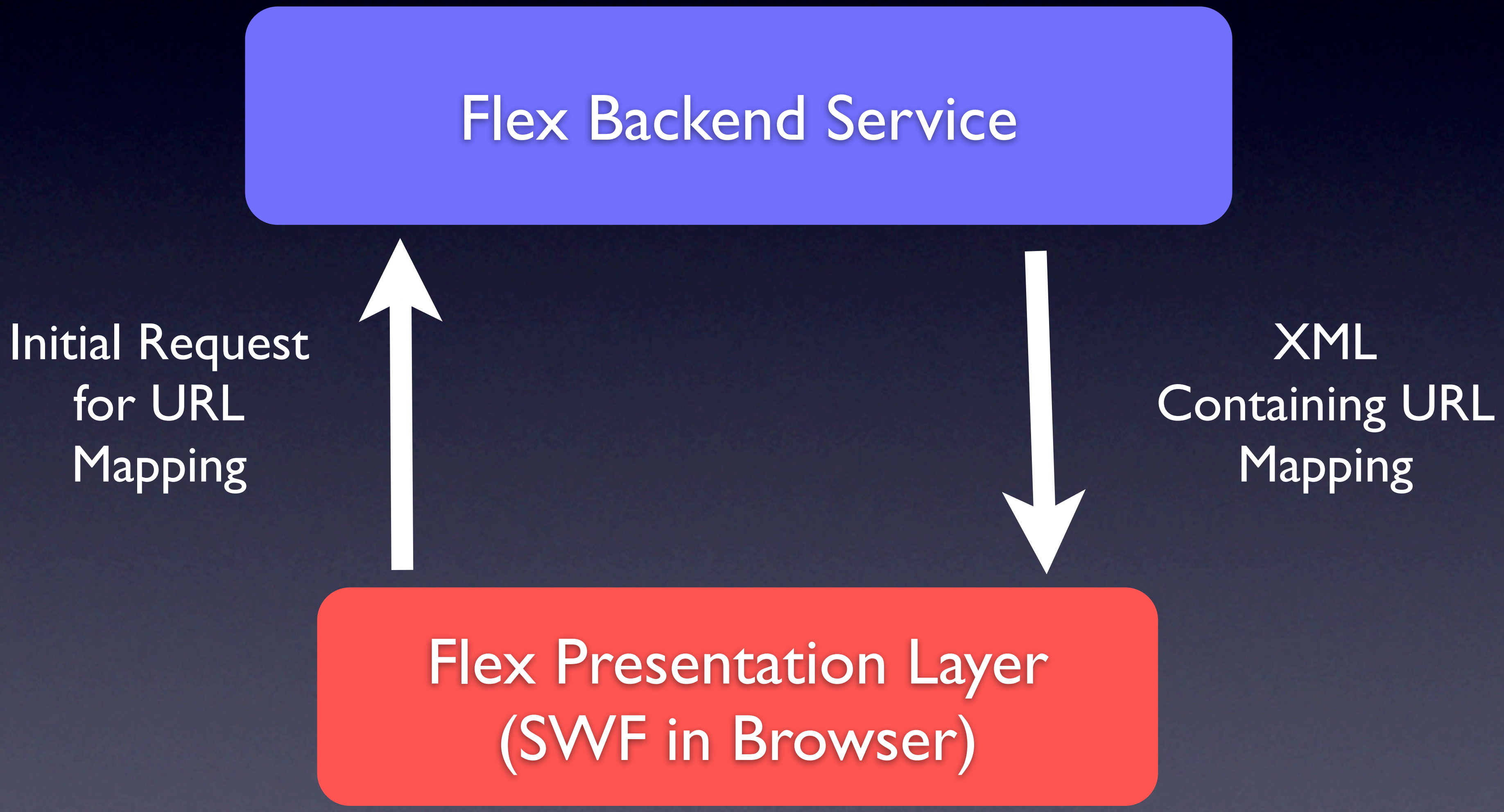
Flex Presentation Layer
(SWF in Browser)

There is absolutely nothing in here!

Script Injection in Flex (cont.)

- Furthermore, Flex can add some additional weirdness that an attacker must work around once a XSS is eventually found:
  - Session-based URL scrambling
  - http://site.com/static/some_stuff.html
  - http://site.com/RANDOM#/CSRF_target

Script Injection in Flex (cont.)



Flex Backend Service

Initial Request for URL Mapping

XML Containing URL Mapping

Flex Presentation Layer (SWF in Browser)

Script Injection in Flex (cont.)

- Browser is allowed to re-fetch mappings
- However, one wrong guess to a URL may de-authenticate your session
- So... on execution, a XSS script must:
  - Fetch the current URL mappings
  - Parse the returned XML for desired actions and *then* execute

Script Injection in Flex (cont.)

- This is kind of like ASLR for web apps... (except that you can just ask the server instead of guessing. So no, not really.)
- OK, but we still need a script injection!
- Where can you find an XSS when all form fields are actually correct?

One Suggestion...

- I noticed a bug in IE when downloading and opening HTML attachments
- Bug can be used to get XSS in Flex (well... only if the site allows user uploads)
- When an HTML file is downloaded and immediately opened in IE, it runs with the script context of the site it was downloaded from!

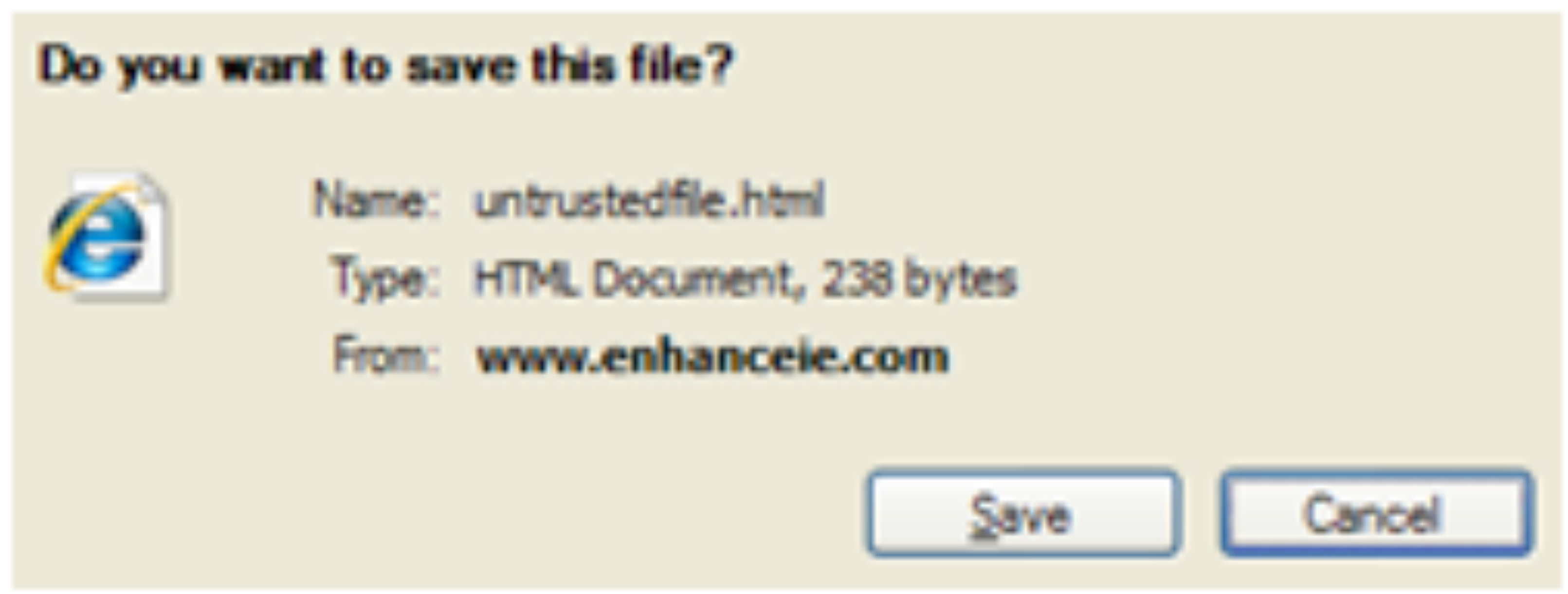
XSS in Flex via IE7

- In Firefox 3, a downloaded HTML file is treated the same as a locally-opened HTML file.
- Kind of lame, but it works good!
- Screencast: awgh.org/iebug

IE8's Solution

- According to the MS Dev Blog, IE8 acknowledges and addresses this issue:
  - Server sets the header "X-Download-Options: noopen"
  - IE8 will then remove the "Open" option from the dialog box.

IE8’s Solution



Do you want to save this file?

Name: untrustedfile.html

Type: HTML Document, 238 bytes

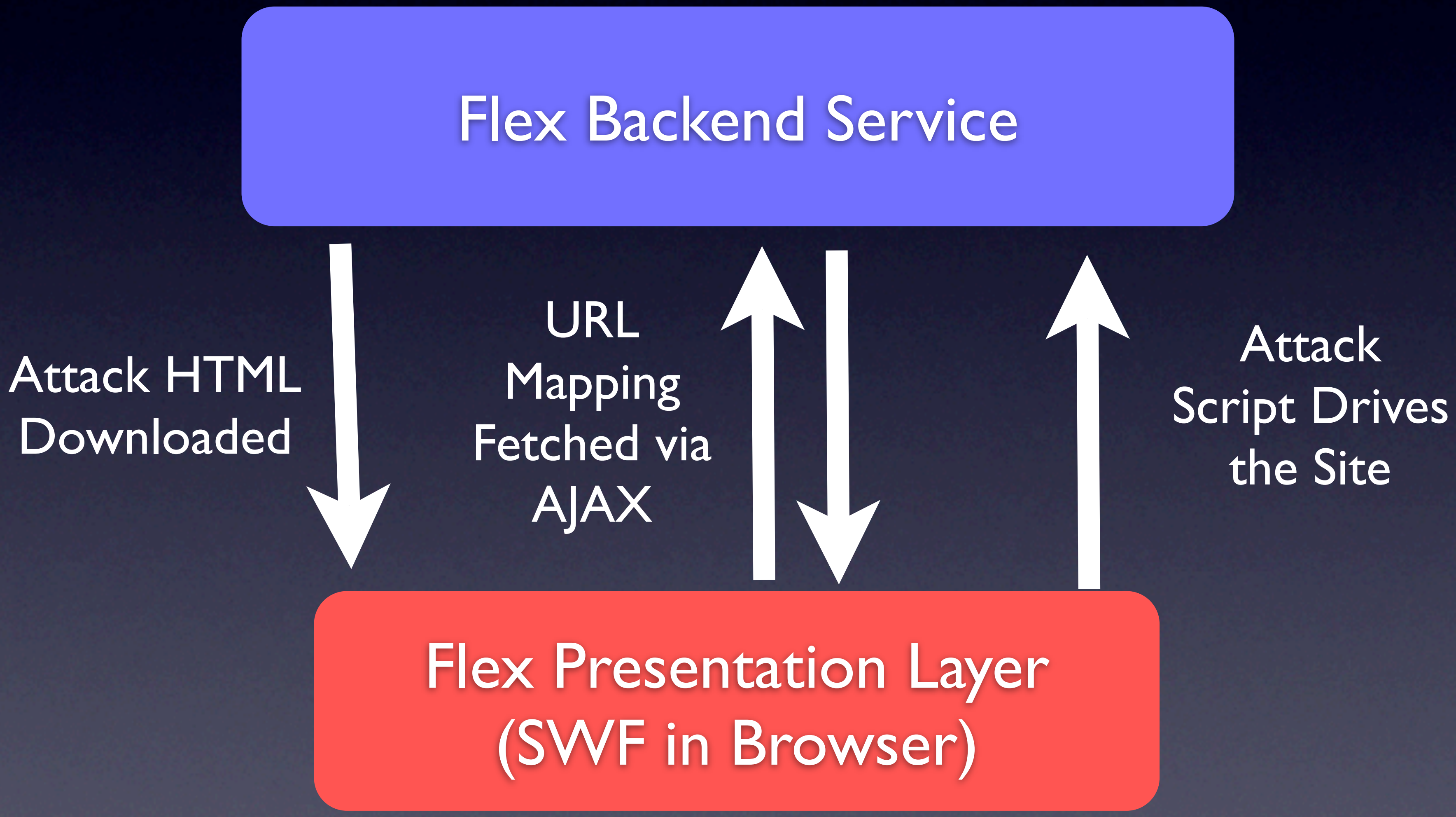
From: www.enhanceie.com

From: http://blogs.msdn.com/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protection.aspx

XSS in IE:

- IE8 will still be vulnerable to this issue if "noopen" is not set by the server
- How many LAMP admins would think to add this to their .htaccess file?
- Although this is a trick for a branch case, it's likely to work for a long while yet

Script Injection in Flex (for real)



Flex Backend Service
Attack HTML Downloaded
URL Mapping Fetched via AJAX
Attack Script Drives the Site
Flex Presentation Layer (SWF in Browser)

awgh.org

• • •

Code Audit - Day One

- grep -lrn “vsnprintf” *
- grep -lrn “strcpy” *
- grep -lrn “malloc” *
- I think we can do a little better...

GCC-Dehydra

- GCC plugin developed by Mozilla
- DIY Static Analysis for free
- Uses the SpiderMonkey JavaScript engine
- Static Analysis may be provably imperfect, but it can still be a little better than Grep

Dehydra > Coverity

- Coverity sold as service:
  - Expensive
  - Closed-source
  - Mixed reviews on track record
- Dehydra developers are super-responsive if you say “I need this feature for security audit”

How does this work?

- Dehydra lets you perform scripted queries on the Abstract Syntax Tree of C++ code
- Scripts are written in JavaScript, which is nice for tree operations
- If you really wanted to, it would be simple to use the same hooks from the gcc-dehydra plugin for a different interpreter

```
function assignVisitor(node) {
  for(var i in node.statements) {
    var loc = node.loc
    var lhs = node.statements[i].type
    var rhs = node.statements[i].assign

    if( rhs && lhs ) {

      if( lhs.unsigned ) {
        if(parseInt(rhs[0].value) > 0) {
          print( "ASSIGN: negative to unsigned at:"+loc+"\n" )
        }
        else if(rhs[0].type && !rhs[0].type.unsigned) {
          print( "ASSIGN: signed to unsigned at:"+loc+"\n" )
        }
      }
      else if(rhs[0].type) {// lhs is signed
        if( rhs[0].type.unsigned ) {
          print( "ASSIGN: unsigned to signed at:"+loc+"\n" );
        }
      }
    }
  }
}
```

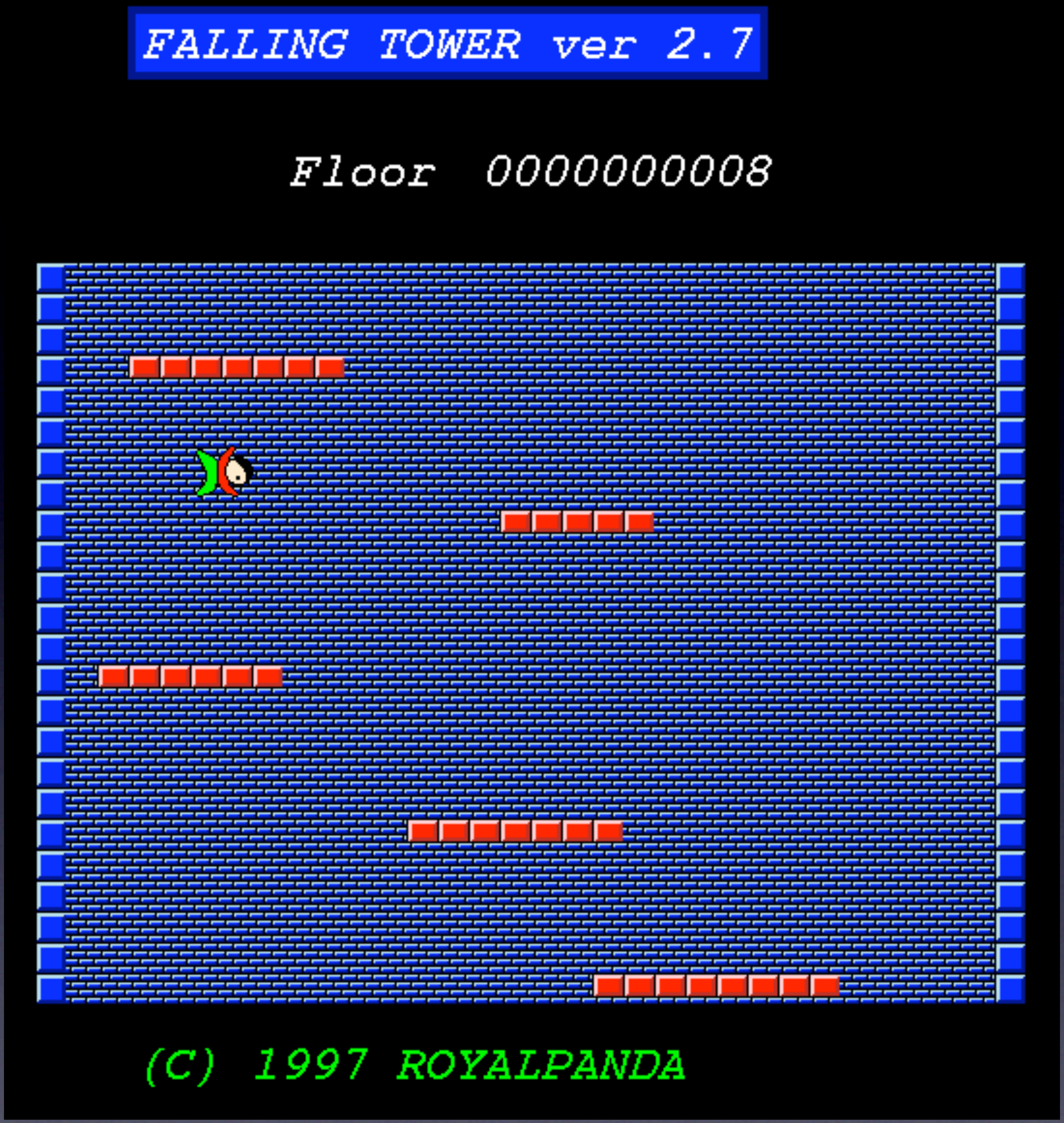
It would be so nice...

Imagine if a bunch of code auditors added common vulnerability scripts to some kind of central repository...

It would be so nice...

Imagine if a bunch of code auditors added common vulnerability scripts to some kind of central repository...

More Time For xjump!



FALLING TOWER ver 2.7

Floor 0000000008

(C) 1997 ROYALPANDA

Next?

One more!

Groo

- Series of scripts that auto-crack WEP keys with Terminal and Web front-ends!
    - Uses 2 Wifi Cards - One Attack, One Admin
    - Prototype unit is on a mini-ITX board with a minimal Gentoo install

Motivation

- My Junk Pile - Made from scrap parts for other projects!
- Can I make something useful by glueing together crap I already have?
- Once you have a box that solves that problem, you’re more likely to use it

ITX & WEP Cracking

- Everyone needs an ITX box that can do Wifi Monitor Mode and Re-Injection.
- Having a box that just does it is the ultimate luxury.
- Really. And it's a chick magnet.

Advantages of ITX

- Relatively small form factors available
- Can use PCI or mini-PCI to get a known-good wireless chipset (ie. Atheros)
- Runs on 12V DC power (like my car battery)
- Other platforms show promise! (eeepc, Atheros AR5315!!!)

Fire and Forget!

- Underlying tech is a horrible kludge of Python, Bash, aircrack-ng tools, and screen!
- Can launch an attack via iPhone, disconnect and come back later!
- I got impatient waiting for someone else to write a good one...

Results

- Average Time-to-Crack a WEP key is 2.5 minutes on a bloody Cyrix C3! (PTW)
- Simple web interface via TurboGears was a good idea - Easily skinnable
- Future Work: Add some Man-in-the-Middle automation and a rogue-AP mode.
- Porting this to my EEEpc during 25c3

All Done