# Bezpečnosť v kontexte RIA


EurOpen

Želiv
5.10. 2011


Mgr. Juraj Michálek

Twitter: http://twitter.com/sinusgear
Blog: http://georgik.sinusgear.com

# Niečo o mne


FACULTAS ARTIS INFORMATICÆ
UNIVERSITAS MASARYKIANA


debian
THE UNIVERSAL OPERATING SYSTEM


Adobe
COMMUNITY
PROFESSIONAL


YSOFT


HTML


georgik's stats
Found: 355 / Hidden: 4
View my profile


jQuery
write less, do more.


open source
initiative


Fx
ADOBE® FLASH® PLATFORM


Java


python™

# Obsah


RIA

Flex, Flash, PDF


HTML5, JavaScript, Mobile

# Rich Internet Applications

Ako to vzniklo?

Výlet históriou

# Rok 2005

Zložitejší JavaScript uvaril browser

# Adobe

3. 12. 2005

Kupuje Macromediu

# FlashPlayer

Najrozšírenejšia platforma

Win, Mac, Lin

# ActionScript 2

S rastúcou aplikáciou

exponenciálne rástla

pracnosť.

# ActrionScript 3 a MXML

Veľmi podobné Jave.

Bez historickej ťarchy Javy.

# Open source framework Flex

Adobe dodáva nástroj

pre vývoj na Flash Platforme.

A definuje skratku RIA.

# Microsoft

Nočná mora web vývojárov: IE6

http://georgik.sinusgear.com/2011/03/05/ie-6-countdown/

# Adobe má úspech

Flash platforma získava popularitu.

# Microsoft

Vidí potenciál a spúšťa Silverlight

# Flash Platforma má náskok

FlashPlayer a ActionScript je starší
a kopec problémov u má vyriešených.

Microsoft sa „inšpiruje“.

# Sun

Silverlight aj Flash vytláčajú Java applety.

Vzniká Java FX.

# JavaFX

Sunu sa nedarí.

Dôležití vývojári odchádzajú do Adobe.

# Apple

iPhone je populárny.

Iná platforma na iPhone predstavuje riziko straty kontroly.

# Adobe Max 2010

Hlavná téma – Flash Player pre iPhone.

Dlho očakávaná novinka.

Bude ohlásené v pondelok
na začiatku konferencie.

# Rana pod pás

V piatok pre Adobe Max
Apple zmení jeden riadok
v licencii

# Zmena

3.3.1 — Applications may only use Documented APIs in the manner prescribed by Apple and must not use or call **any private APIs**. Applications must be originally written in Objective-C, C, C++, or JavaScript as executed by the iPhone OS WebKit engine, and only code written in C, C++, and Objective-C may compile and directly link against the Documented APIs (e.g., **Applications that link to Documented APIs through an intermediary translation or compatibility layer or tool are prohibited**).

# FP pre iPhone

Zostáva v labáku Adobe.

Než Apple zmení svoje rozhodnutie.

# iPad a iPhone

Jobs hlása: HTML5 je tá správna cesta

# Google

Úzko spolupracuje s Adobe.

Zabuduje Flash Player do Chromu.

Zároveň výrazne zlepší podporu JavaScriptu.

# Vic Gundotra - Google

The platform that is not owned by anyone

truely belongs to everyone.

HTML5

# A znova objavenie kolesa

HTML5 reimplemetuje nanovo väčšinu vecí z FP.

# Otvorený kód

Flex – postupne uvoľnený pod Mozilla Public Licence

Silverlight

JavaFx

# Flash Builder


Eclipse based

študenti a akademický pracovníci
- licencia zdarma

# MXMLC, COMPC

shell, ant task

FlexMojos – Maven
(Lin, Win, Mac, BSD)

Intellij Idea (Ultimate)

# Architektúra RIA aplikácii

Paralela s desktop aplikáciami

Jeden kód v pamäti

Komunikácia cez API

# Permanent cookie

FP si udržiaval vlastné cookie.

Security issue.

# FP 10.3

Mazanie cookie je konečne možné kontrolovať.

# Crossdomain

FP umožňuje GET a POST.

Obmedzenie: rovnaká doména

# Prístup na iné domény

crossdomain.xml v roote webu

FP ho kontroluje predtým, než odošle požiadavku.

# crossdomain.xml

```
<cross-domain-policy>
   <allow-access-from  domain="*"/>
   <allow-http-request-headers-from  domain="*" />
</cross-domain-policy>
```

# REST

GET a POST
odosielané cez browser

PUT, DELETE atp. sú blokované

# Hlavičky request/response

FP dokáže vytvoriť niektoré hlavičky.

Nedokáže však načítať žiadne.

# Flash Player Sockets

Priamy prístup k socketu.

Od FP 9.0.124

# Socket Policy

Socket Policy File Server

port 848

# Policy document

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<site-control permitted-cross-domain-policies="master-only"/>
<allow-access-from domain="swf.example.com" to-ports="123,456-458" />
</cross-domain-policy>
```

# Za firewallom

848 je blokované...

A sme došli stará mama.

# Prístup k súborom

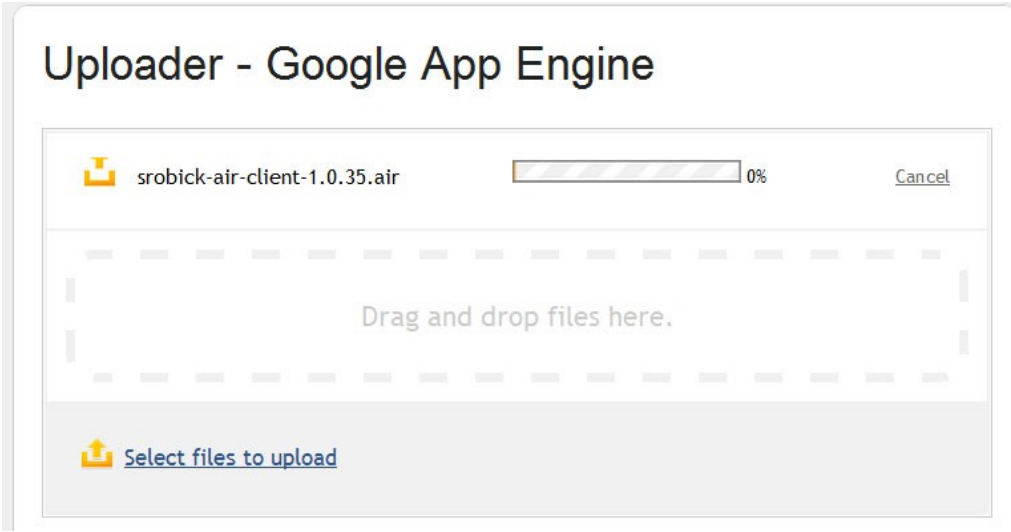
Otvorenie dialógu pre výber súboru

je možné len ako reakcia na uživateľskú

udalosť.

Click :-)

# File Uploader



www.klokantech.com

# Transparent SWF

Overlay

this.parentApplication.alpha = 0;

# SWF

SWF obsahuje bajtkód.

Ten je možné dekompilovať.

# Assety v SWF

Zo SWF je možné vytiahnuť

súbory.

# Obfuskácia

Je možná.

Silnejšie riešenie: enkrypcia
(Nitro LM)

# HTTPS

Server MUSÍ mať validný ceritikát.

# HTTPS a IE

Warning pri každom requeste.

# HTTPS a Google App Engine

Certifikát zdarma.

Plne validný len na jednu úroveň.
https://srobick-server.appspot.com/

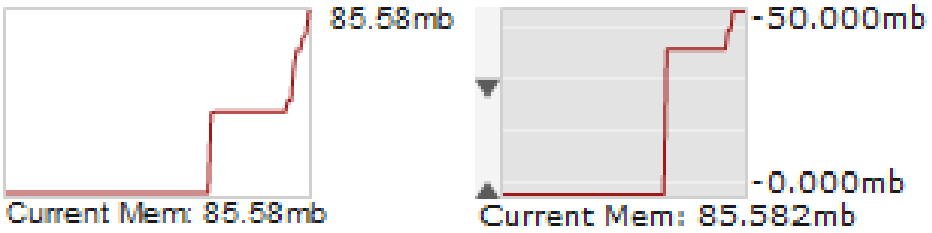
Podúrovne sú nevalidné.
http://test.srobick-server.appspot.com/

# Certifikát

Zdarma (slabší)

www.startssl.com

# Memory Leak - Flash




## Monitoring Flash Player pamäte

http://georgik.sinusgear.com/projects/flash-memory-monitor/

Loitering Objects

# Bezpečnostné opravy

Pre administrátorov: Aktualizujte!

Security oprava je vydaná pomerne rýchlo od objavenia hrozby.

Adobe Security Bulletin
http://www.adobe.com/support/security/

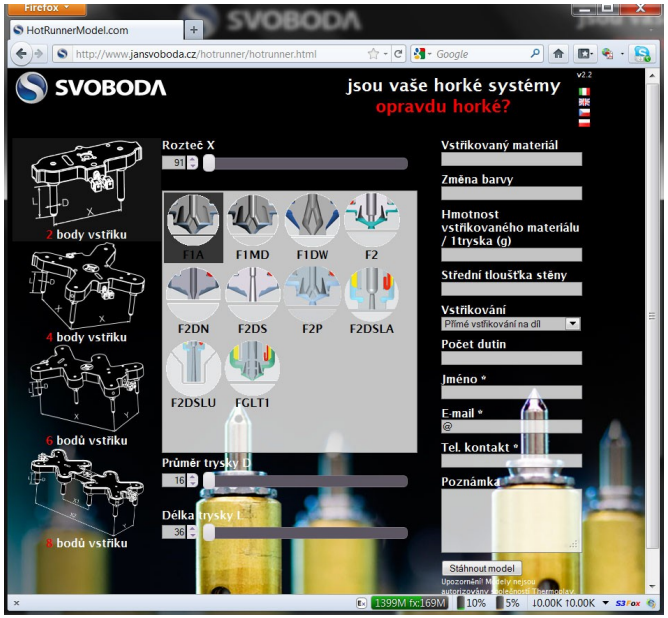
# Bug reporting

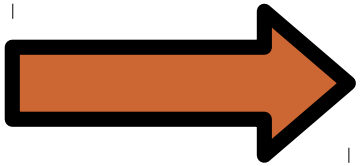
https://bugbase.adobe.com/

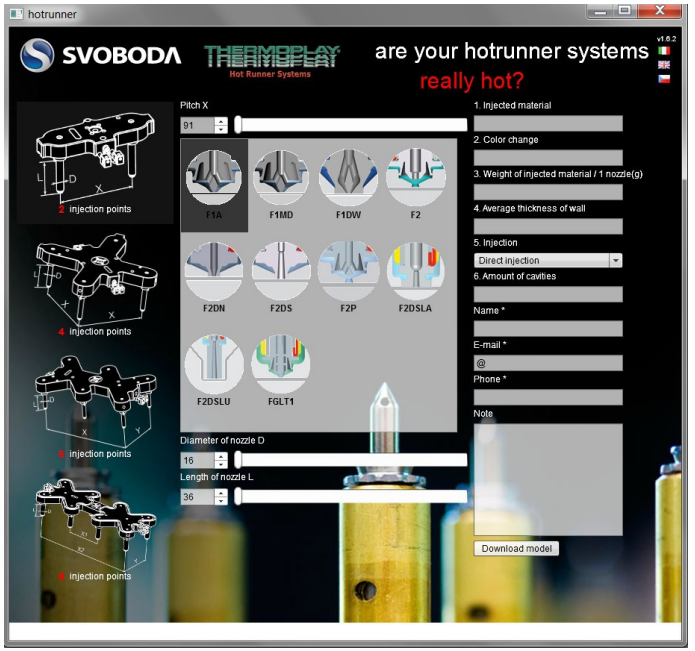
# RIA z webu na desktop

Zoberme web app.
Nech je z nej desktop app!

www.hotrunnermodel.com





# AIR Runtime

„Upravený“ FP pre desktop.

Flex SDK + AIR rozšírenia

Win, Lin, Mac, Mobile

# RIA z webu na mobil a TV

Jeden kód, jeden runtime
a množstvo cieľových platformiem:

Mac, Win, Lin, Android, iOS, BlackBerry

# Odstránené obmedzenia FP

Crossdomain nemá význam.

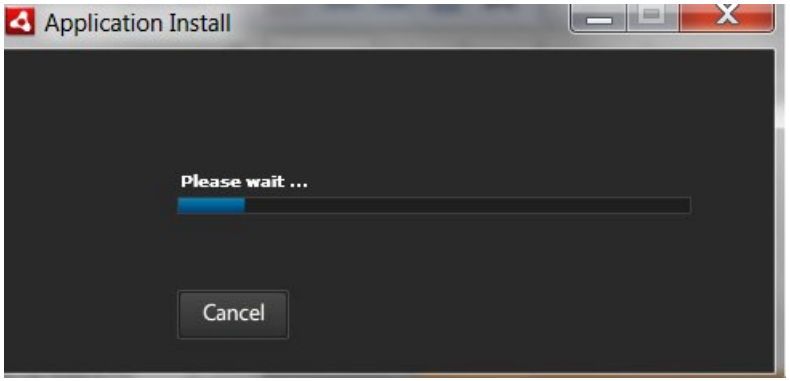
Socket priamy prístup.

Prístup na súborový systém.

# AIR aplikácia - manifest

```
<allowBrowserInvocation>true</allowBrowserInvocation>
```

# AIR update aplikácií



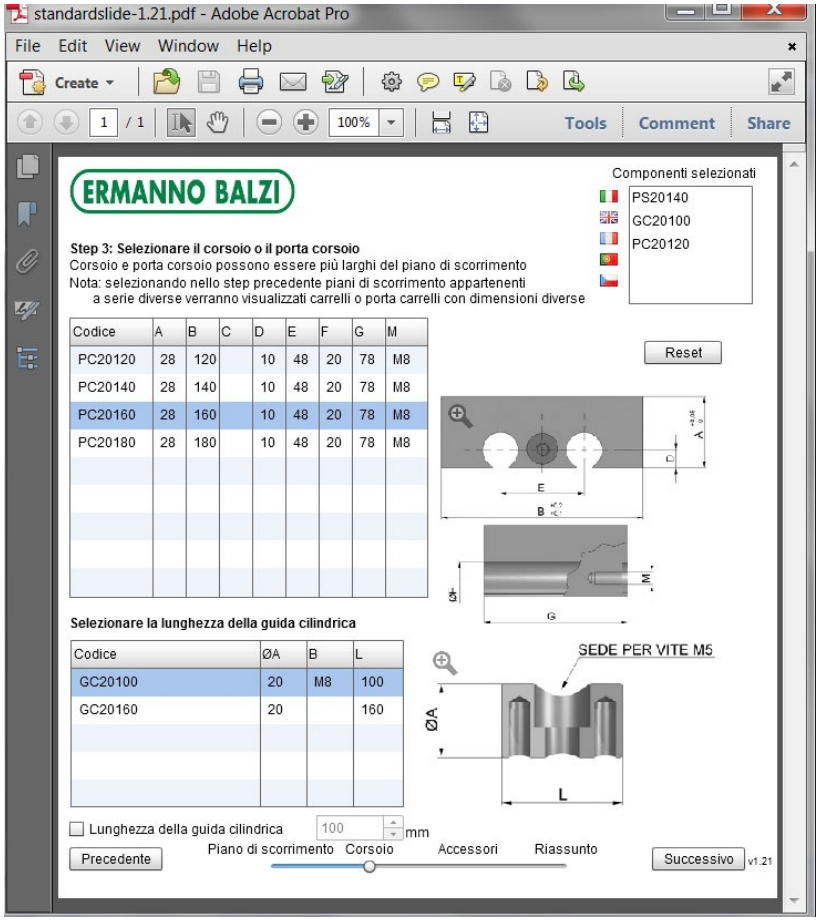

# AIR a HTTPS

Platí to isté čo pre web.

Certifikát musí byť validný.

Inak čo request to warning.

# RIA v PDF




Aplikácia zabalená do PDF.

# Security Sandbox

Každá požiadavka mimo sandbox
si vyžiada potvrdenie.

# Projekt Rome


Tvorba interaktívneho PDF

http://rome.adobe.com

# Kontinuálna integrácia

Jenkins

Príklad - Open Source AS3/MXML projekty:

http://ci.sinusgear.com

# Silverlight

Konkurent Flexu a FP

Aktuálne zameranie WP7

# Komunikačné protokoly

Nad HTTP

XML

SOAP

JSON

AMF3

# XML a SOAP

Penalizácia (de)serializácie.

# AMF3

Binárny protokol.

Veľmi rýchly a otvorený.

Klient FP only, server Java only.

# AMF3 introspection

Toaster Lite

Dekódovacia proxy

http://georgik.sinusgear.com/2011/01/14/how-to-introspect-amf-communication/

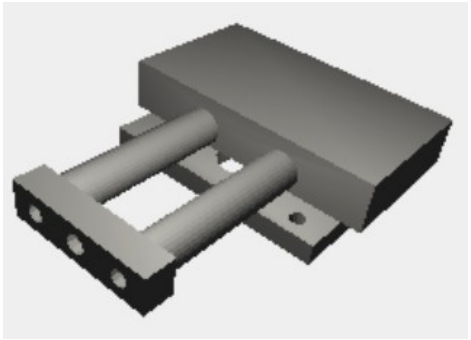
# JSON

Rýchlosť, otvorenosť, čitateľnosť.

F12

# HTML5, JavaScript

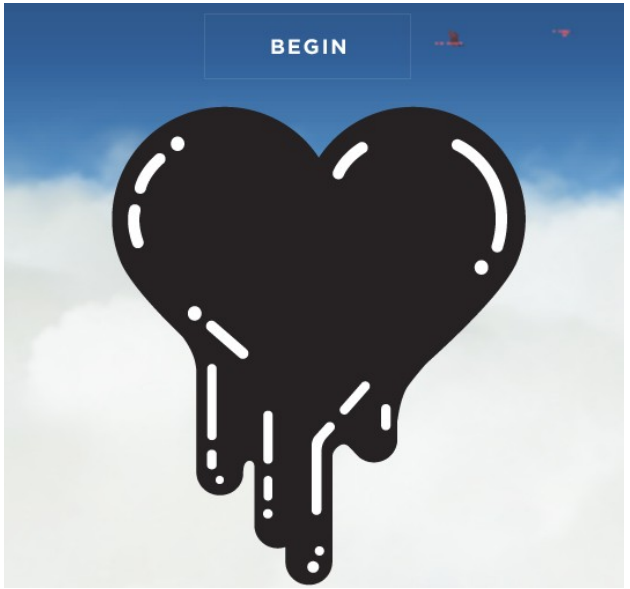
# Canvas, WebGL



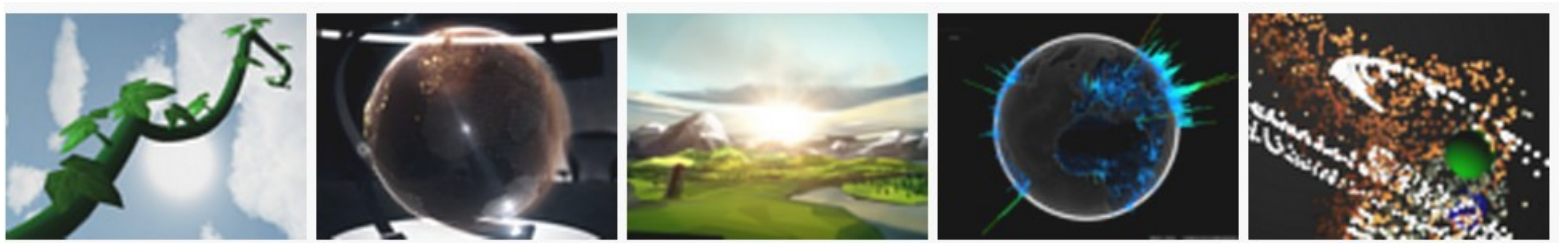
http://www.ermannobalzi.com/app/standardslide-2.0/


http://www.webglearth.org/

http://www.ro.me/



# three.js



https://github.com/mrdoob/three.js/

# jQuery a jQueryMobile


Fenomenálny prielom v možnostiach JavaScriptu.

```
$("#zeliv").animate({top:"300px"}).animate({left:"10px"});
```

# Malý web server

python -m SimpleHTTPServer

# EmglareMobile


App: http://www.emglare.com

Mobile app: http://m.emglare.com

Postavené na PhoneGap

# Dreamweaver a PhoneGap

Deployment na Android

# Back button

Užívateľ sa môže vrátiť k predchádzajúcej aplikácii.

Nutné zneplatniť citlivé data.

# GET

Pozor! Na keš.

Každý browser sa chová inak.

POST sa nekešuje.

# Crossdomain

GET/POST request je obmedzený na doménu.

# Sanitizácia HTML

Príklad: diskusný portál

vkladá do stránky nesanitizované príspevky

<script.....>

# JSON problém

Incident s Gmailom (fixed)

<script src="http://gmail.com..."></script>

# Ochrana dát proti crossdomain

**while (true);** &&&START&&&{"Success":true,"

# User Tacking DOM

```
$("body").mousemove(
    function(event){
        insertData(event.pageX,event.pageY,event.clientX,event.clientY);
    }
);
```

# Ochrana JavaScriptu?

Aspoň kompresia

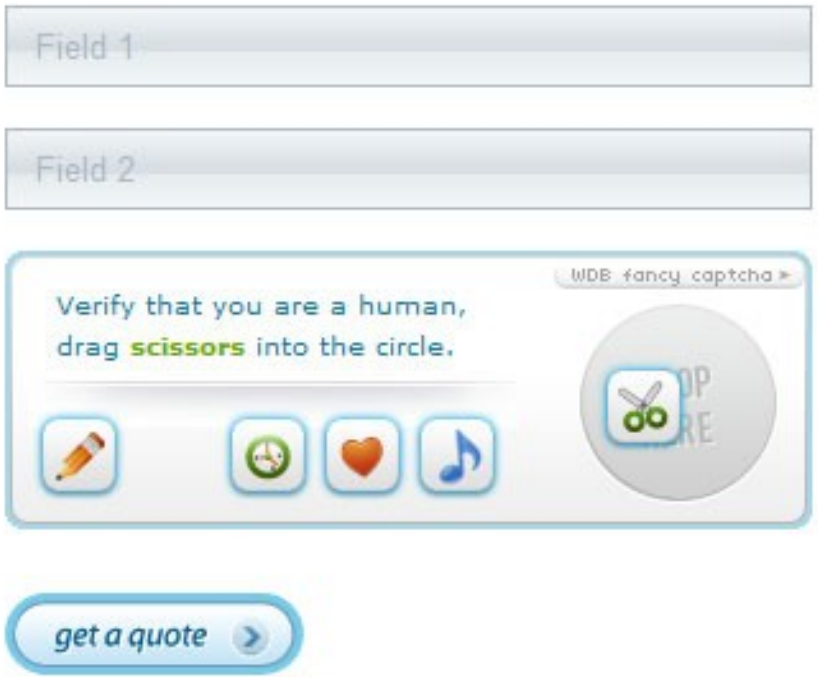
YUI-Compressor

http://developer.yahoo.com/yui/compressor/

# Memory leak

JavaScript - Circular reference

# Captcha :-D




http://www.webdesignbeach.com/beachbar/ajax-fancy-captcha-jquery-plugin

# Bezpečnostné výstrahy pre SW

The Open Source Vulnerability Database

http://osvdb.org/

# $(this).close()


Europen

Želiv
5.10. 2011


Mgr. Juraj Michálek

Twitter: http://twitter.com/sinusgear
Blog: http://georgik.sinusgear.com