# OWASP GÖTEBORG

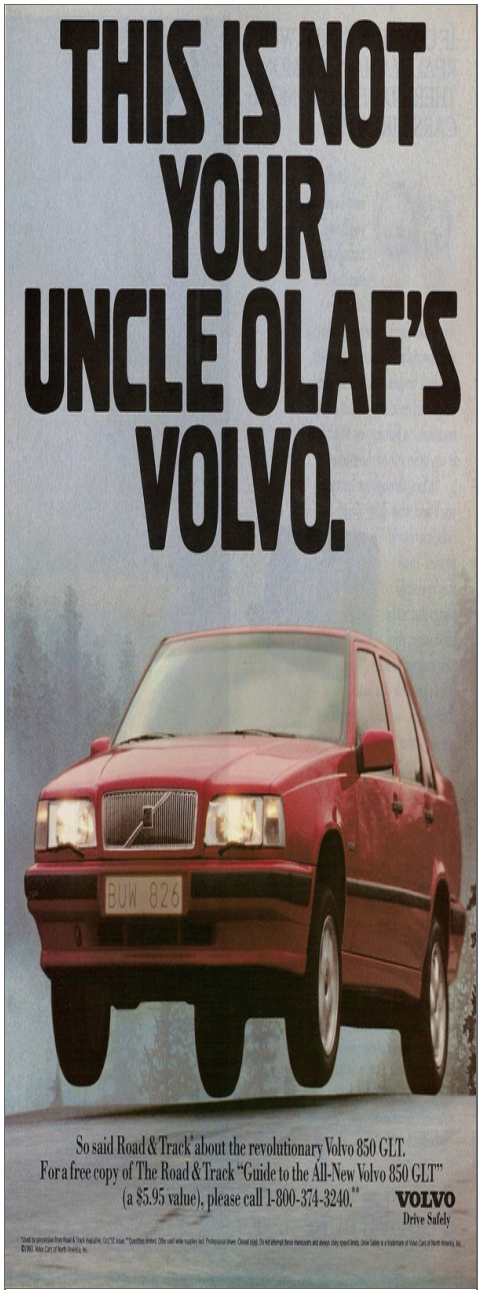
## SEPTEMBER 2012

## HYBRID MOBILE APPS & THE EVOLVING WEB

BY MIKKO SAARIO

***Twitter: @midisFI***
***(http://twitter.com/midisfi)***

# THIS IS NOT YOUR UNCLE OLOF'S
"OWASP TOP 10 MOBILE SECURITY"
# TALK



# AGENDA

1. Hybrid environments & the Open Web Platform
    - Hybrid environments mix HTML+JS with Native code
    - OWP + a peek into stuff like getUserMedia
    - 30 min or so
2. Case review from the mixed world
    - Security evaluation of a new multi-technology application
    - 10 min or so
3. Security and Agile development - do they mix?
    - A bit of theory
    - And a bit of practice - 1st hand
    - 20 min or so

# Oh well

**Jeremiah Grossman** @jeremiahg

If you submit an InfoSec preso on "mobile", "cloud", or "agile"... youve GOT to differentiate. Hundreds of others are covering the same topic.

Expand

# Almost got a 'Bingo'

# ME

- Nokia
- Security manager for Sales & Marketing services
- Founder of OWASP Helsinki
- Motto: "the more you learn, the less you seem to know"
- More of a Defender & Breaker than a Builder

POLL

DISCLAIMER

# Examples

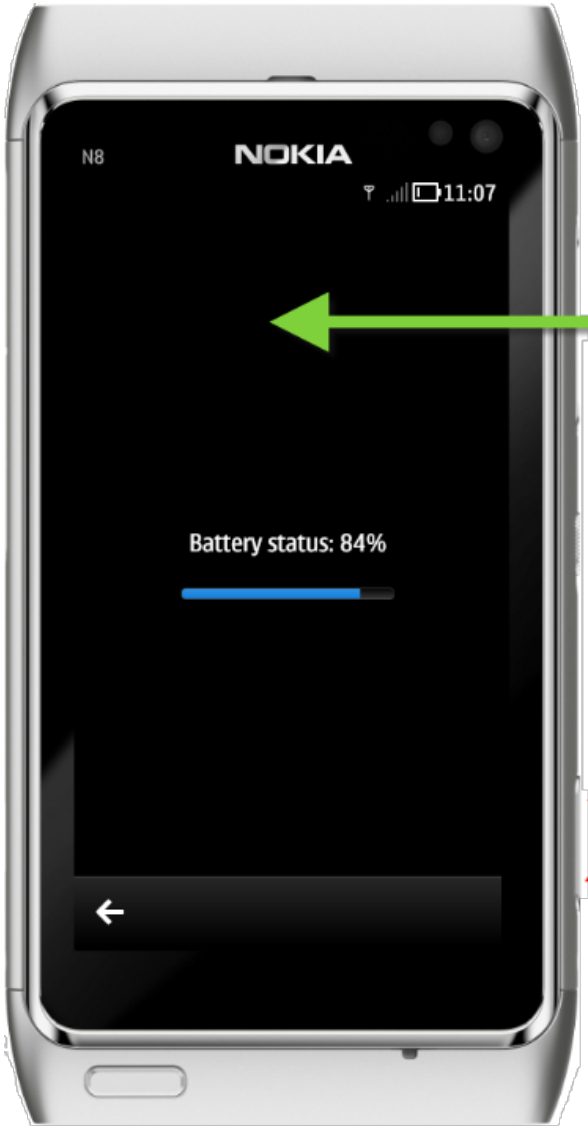
Are for Windows Phone 7.5
with an odd Qt/QML one thrown in

Android and iPhone guys - just be cool

# TRADITIONAL AIR GAP

## A PRETTY EFFECTIVE SECURITY CONTROL

# WEB HAD NO ACCESS TO DEVICE API




Native

```
void MainWindow::showExpanded()
{
#if defined(Q_OS_SYMBIAN) || defined(Q_WS_SIMULATOR)
    showFullScreen();
#elif defined(Q_WS_MAEMO_5)
    showMaximized();
#else
    show();
#endif
}

void MainWindow::setupGeneral()
 {
     deviceInfo = new QSystemDeviceInfo(this);

     ui->batteryLevelBar->setValue(deviceInfo->batter

     connect(deviceInfo, SIGNAL(batteryLevelChanged(i
             ui->batteryLevelBar, SLOT(setValue(int))
 }
```

HTML

X

```
<!DOCTYPE html>
<html>
<head>
  <title>Battery Status API Example</title>
  <script>
    var battery = navigator.battery;

    battery.onchargingchange = function () {
      document.querySelector('#charging').textConter
    };

    battery.onlevelchange = function () {
      document.querySelector('#level').textContent
    };

    battery.ondischargingtimechange = function () {
      document.querySelector('#dischargingTime').tex
    };
  </script>
</head>
<body>
  <div id="charging">(charging state unknown)</div>
  <div id="level">(battery level unknown)</div>
  <div id="dischargingTime">(discharging time unknov
</body>
</html>
```

# SECURITY USED TO BE

## SIGNING APPS WITH CAPABILITIES

Permission, privilege, you name it…
So, installation handled the "rights"

## BUFFER OVERFLOWS

## SMS OF DEATH

## MALWARE

## AND SO FORTH

# AND STILL IS...

## THEY DIDN'T DISAPPEAR

# BRIDGING THE AIR GAP #1

NATIVE += WEB

HYBRID

# LET'S ADD A WEBVIEW

```
import QtWebKit 1.0

WebView {
        url: "https://www.owasp.org"
        preferredWidth: 490
        preferredHeight: 400
        scale: 0.5
        smooth: false
}
```

Code: Qt/QML

# MAGIC HAPPENS

# A HYBRID ENVIRONMENT

- Native mobile apps utilize Web technologies inside the app
  - HTML, CSS and JavaScript embedded in / utilized by native code (C#, VB, objective-C, C++, "java")
- Typically utilizing

```
/(ui)?Web(View|Browser)/g class
```

  For the rest of us: a "WebBrowser", "uiWebView", or just plain "WebView"

  - Windows Phone 7: WebBrowser control
- Rendering engine without the "chrome" (Browser UI)

# COMMON

- Qt/QML multiplatform
- Widgets
- Android
- Mac OS X, iOS
- Windows OS / Phone
- Apache Cordova / PhoneGap

# NATIVE AND JS CAN TALK

## In native, expose an interface to JS

```
<phone:WebBrowser

ScriptNotify="alert_ScriptNotify"
IsScriptEnabled="True"
/>
```

## Javascript calls the parent native app

```
function AlertSilverlight(data)
{
        window.external.notify(data);
}
AlertSilverlight(1);
```

## Listener picks it up and executes

```
private void alert_ScriptNotify(object sender, NotifyEvent
Args e)
{
        MessageBox.Show(e.Value);
}
```

Code: WinPhone 7 C#/Silverlight/XAML/JavaScript

# SECURITY FUNDAMENTALS

# OWASP TOP TEN

YES, IT'S ALL VERY VALID

BOTH OF THEM

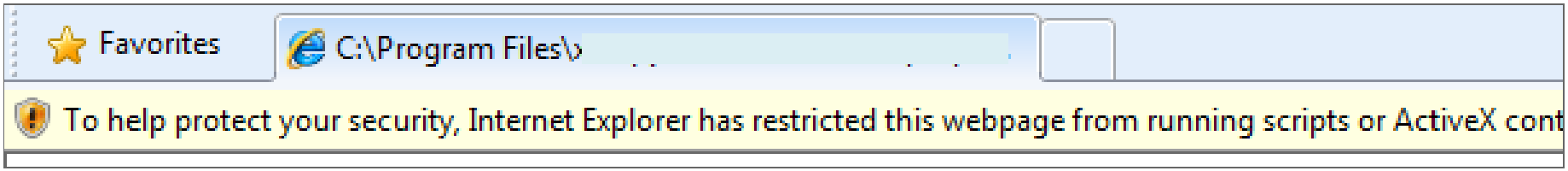
# UI CONTROLS

A lot of the usual UI controls are missing

E.g. WP7 will silently fail self-signed, untrusted SSL cert

No SSL "lock" visible

Warnings, popups etc.



# SAME ORIGIN POLICY

Notes for Windows Phone 7

- Content loaded from isolated storage is not restricted by SOP (file:///)
- Content created via NavigateToString is not restricted by SOP

```
var html = "<html><script>...code...</script></
html>"

webBrowser1.NavigateToString(html);
```

- JavaScript called via InvokeScript can be from any domain
- Some difference on desktop vs mobile

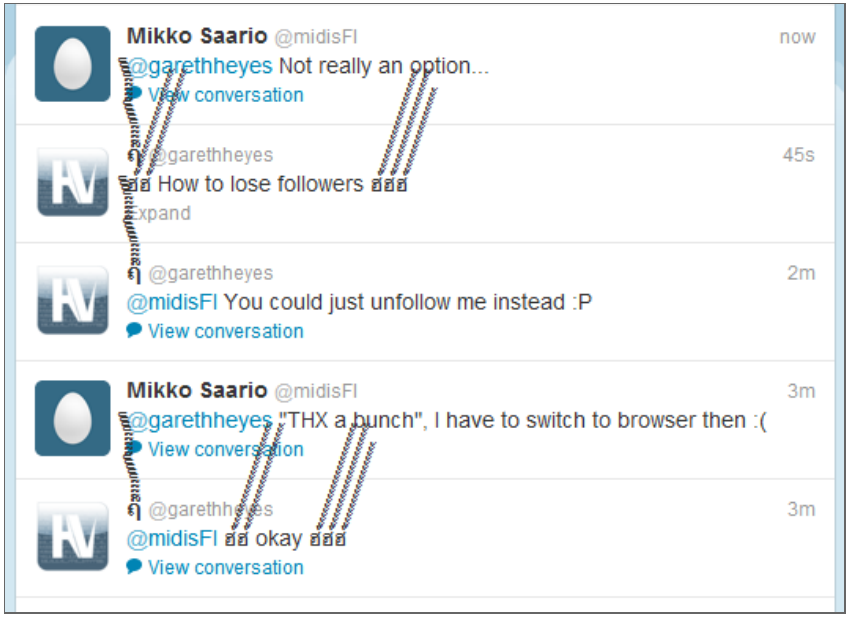
## E.G. QT HAS SOP LIMITS ON FILE:///

# EVAL IS STILL EVIL

## ARE YOU EVAL'ING SOME INPUT?

eval(), setTimeout(), setInterval(), new Function()

# BUFFER OVERFLOWS




# THE ABOVE KILLED N9 TWITTER CLIENT (QT & C++)

```
we can't know how much space we need to allocate...
...for this pathological string we are generating
two glyphs for each character.
```

# INJECTIONS

- SQL injection
- XML Query / XPath injection

  Using XQuery or XPath dynamically with user-supplied input could leave you vulnerable in Qt

  Use bound parameters

# DENIAL OF SERVICE

Isolated storage on WP7 has no size restrictions
So one app may fill up the whole storage space

# CONFIGURATIONS

Define your environment specs

Your mileage will vary greatly

Each framework has their own details

# SCRIPTING

```
/* Qt default: true */
QWebSettings::JavascriptEnabled

QWebSettings::JavascriptCanOpenWindows
QWebSettings::JavascriptCanAccessClipboard

<!-- Windows Phone 7 default: disabled -->
<Grid x:Name="LayoutRoot">
        <phone:WebBrowser Name="mybrowser"
                IsScriptEnabled="True"
                Source="index.html"
                ScriptNotify="pokeMyScript" />
</Grid>
```

# PLUGINS

Java, Flash and other plugins

```
/* Qt; No plugins in WP7 */
QWebSettings::JavaEnabled
QWebSettings::PluginsEnabled
```

# ETC.

- Configure cross-domain actions

```
QWebSettings::XSSAuditingEnabled
QWebSettings::LocalContentCanAccessRemoteUrls

QWebSettings::LocalContentCanAccessFileUrls
/* can qrc:// access file:// */
```

- Anything else that is configurable

```
QWebSettings::PrivateBrowsingEnabled
QWebSettings::DeveloperExtrasEnabled

IsGeolocationEnabled = "true"
```

# DEMO TIME

## A WP7 DEMO APP

# BRIDGING THE AIR GAP #2

## OPEN WEB PLATFORM / HTML5

# OPEN WEB PLATFORM

- HTML5 (of course)
- Web APIs
- DOM
- CSS
- SVG
- MathML
- WebRTC
- Device APIs
- EcmaScript / JavaScript
- HTTP, URI
- Media Accessibility Checklist
- etc.

# WebRTC

## WEB REAL TIME COMMUNICATIONS

- MediaStream (getUserMedia)
  - Access to e.g. device camera and microphone
- PeerConnection (peer-to-peer connections)
  - Enables e.g. VoIP from browser to browser (using ICE + STUN & TURN servers)

...lets look at getUserMedia in a moment

# Web APIs

- Clipboard API
- File API
- Fullscreen
- Gamepad
- Indexed DB
- Pointer Lock
- Web Workers
- XHR2 (CORS) etc. etc. etc.

**Boot to Gecko**
**(https://wiki.mozilla.org/WebAPI)**

# Device APIs

- Battery Status
- Calendar API
- Contacts API
- Device Orientation API
- Geolocation + level 2
- Media Capture (gone)
- Vibration API etc. etc.

# Remember the Good Old Flash Camera Snooping Days?

Are they coming back?

# getUserMedia
## Hello, World!

img source: http://safeandsavvy.f-secure.com

# BLEEDING EDGE

CHROME 21

FIREFOX 16+

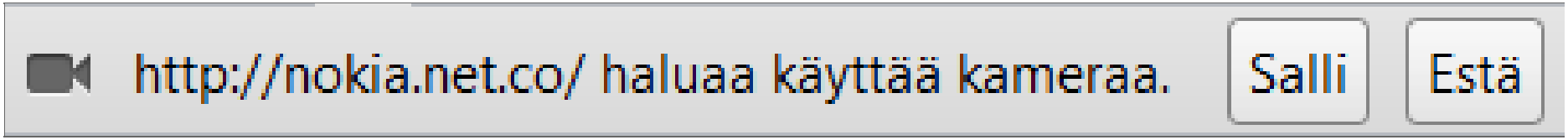
OPERA 12

OPERA MOBILE 12

{ ANDROID > SYMBIAN }

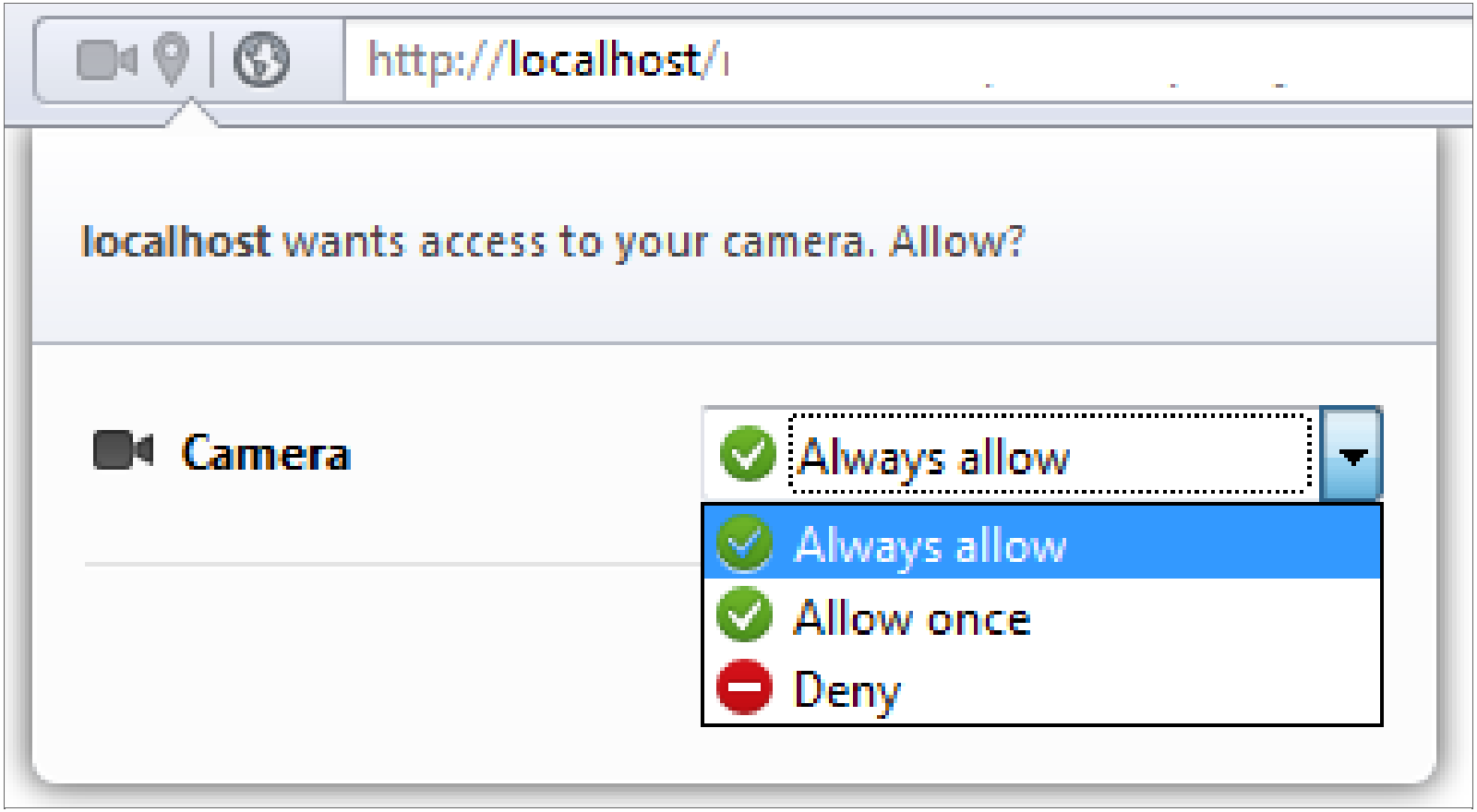
# NU SKA NI FÅ LÄRÄ ER LITE FINSKA

CHROME 21




JA / NEJ

OPERA 12


http://localhost/
localhost wants access to your camera. Allow?
Camera
Always allow
Always allow
Allow once
Deny

# FIREFOX 15

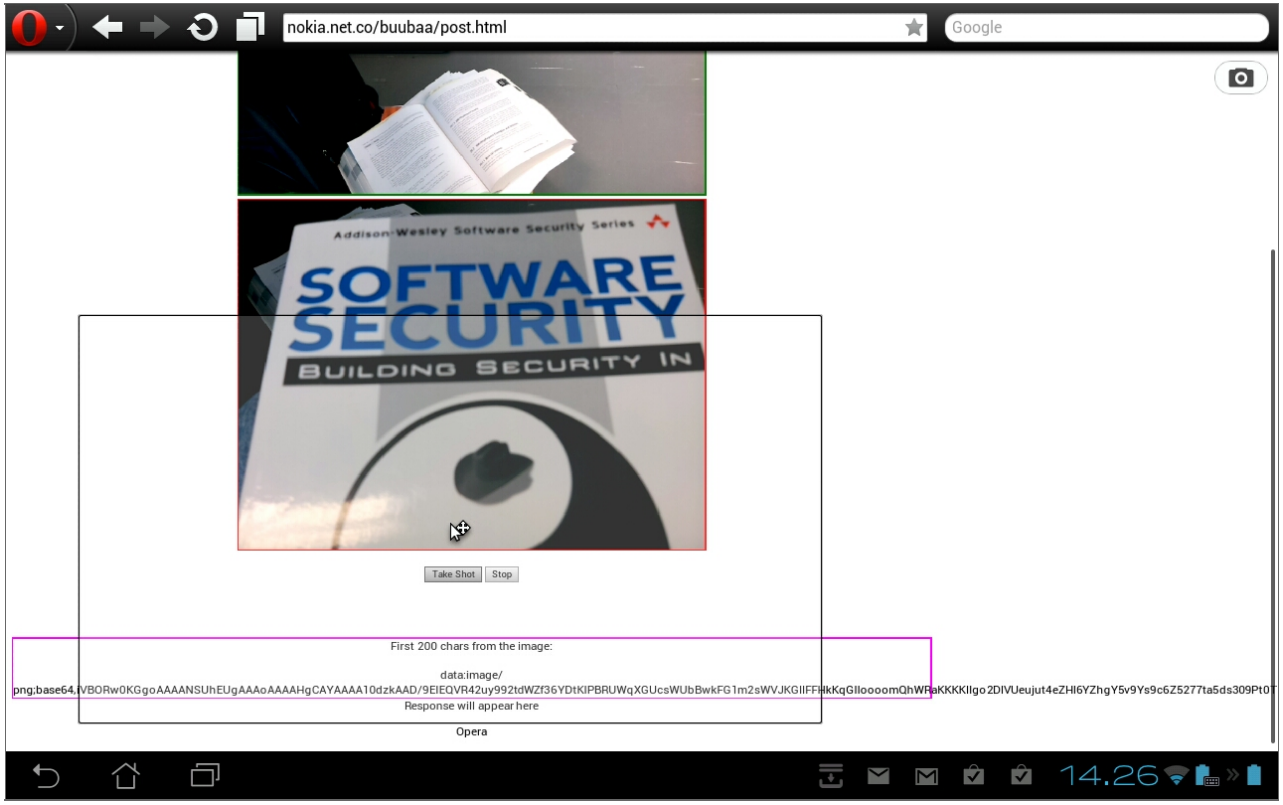
## OOPS NO GO :)

Looks more like **FF 16 & 17**
**(http://alexandre.alapetite.fr/doc-alex/html5-webcam/)**

# DEMO2 TIME

## GETUSERMEDIA ON A STANDARD BROWSER

# ANDROID 4.0 ICS


nokia.net.co/buubaa/post.html
Google
Addison-Wesley Software Security Series
SOFTWARE SECURITY
BUILDING SECURITY IN
Take Shot
Stop
First 200 chars from the image:

# IFRAME CAMERA

```
W3C proposal & current implementation:
--------------------------------------
In order to prevent unexpected behaviour and to stay on the safe
side of user's privacy, it may be useful to explicitly mention in
the specification that calls from s be silently denied.
.
.
.
"No conclusion"
```

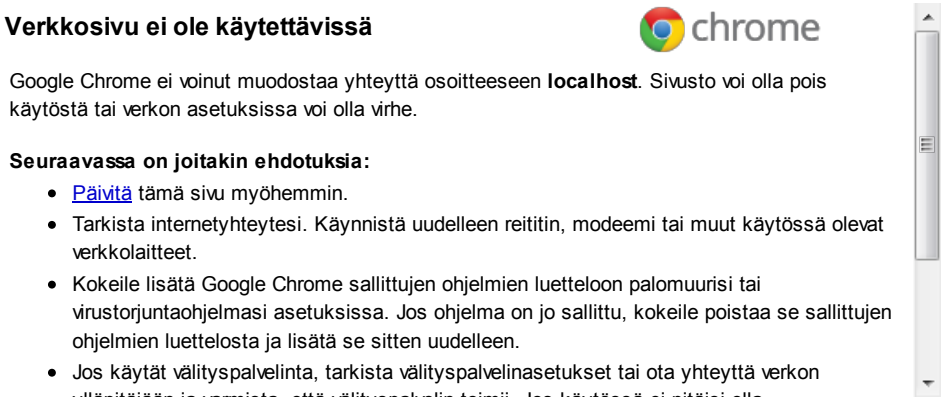
**W3C site**
**(http://www.w3.org/wiki/Media_Capture#iFrame_behavior)**

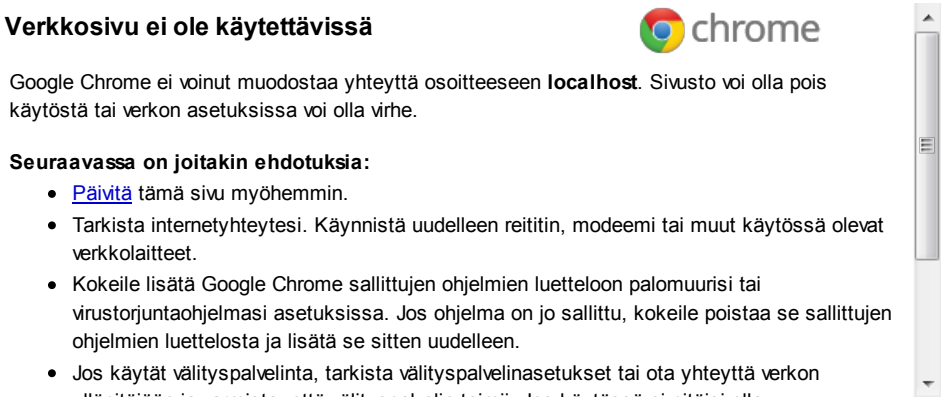
# FILE API

## SANDBOXED LOCAL FILESYSTEM

`filesystem:http://localhost/temporary/`

# DEMO


Verkkosivu ei ole käytettävissä
chrome
Google Chrome ei voinut muodostaa yhteyttä osoitteeseen **localhost**. Sivusto voi olla pois käytöstä tai verkon asetuksissa voi olla virhe.
**Seuraavassa on joitakin ehdotuksia:**
Päivitä tämä sivu myöhemmin.
Tarkista internetyhteytesi. Käynnistä uudelleen reititin, modeemi tai muut käytössä olevat verkkolaitteet.
Kokeile lisätä Google Chrome sallittujen ohjelmien luetteloon palomuurisi tai virustorjuntaohjelmasi asetuksissa. Jos ohjelma on jo sallittu, kokeile poistaa se sallittujen ohjelmien luettelosta ja lisätä se sitten uudelleen.
Jos käytät välityspalvelinta, tarkista välityspalvelinasetukset tai ota yhteyttä verkon


Verkkosivu ei ole käytettävissä
chrome
Google Chrome ei voinut muodostaa yhteyttä osoitteeseen **localhost**. Sivusto voi olla pois käytöstä tai verkon asetuksissa voi olla virhe.
**Seuraavassa on joitakin ehdotuksia:**
Päivitä tämä sivu myöhemmin.
Tarkista internetyhteytesi. Käynnistä uudelleen reititin, modeemi tai muut käytössä olevat verkkolaitteet.
Kokeile lisätä Google Chrome sallittujen ohjelmien luetteloon palomuurisi tai virustorjuntaohjelmasi asetuksissa. Jos ohjelma on jo sallittu, kokeile poistaa se sallittujen ohjelmien luettelosta ja lisätä se sitten uudelleen.
Jos käytät välityspalvelinta, tarkista välityspalvelinasetukset tai ota yhteyttä verkon

# CHROME APPS

- Apps run outside "chrome browser", no browser UI
- But made with html, js & css
- "Offline", but appear like native apps
- Quite strict security model:
  - Mandatory strict CSP
  - Prevents inline scripts, eval & "new Function()"
  - Those can be used in a sandboxed (iframe) page
  - <browser> tag to safely display web content
  - Accept permissions at installation
  - Each window can have separate privileges (reduce attack surface)
  - Process and storage isolation
  - Access ext content, but e.g. xhr requires whitelisting the site
- New APIs to access OS: bluetooth, usb etc.

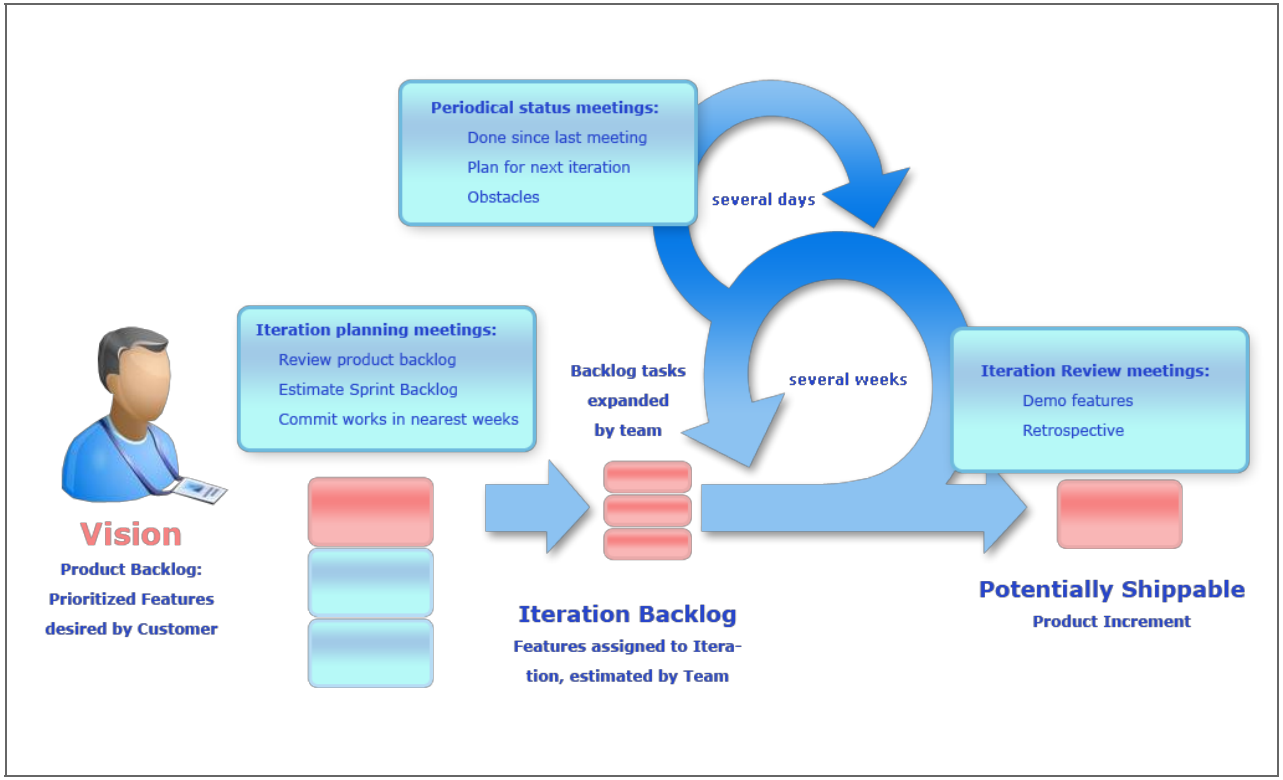
END OF PART 1

# CASE STUDY

# AGILE

## EXPERIENCES WITH AGILE TEAMS

# THEORY




Proudly reused from: www.digdes.com

# KEY CONCEPTS

- Epics, user stories and features
- Abuse stories
- Sprint vs Product backlog
- Sprint review & Definition of Done
- Tools, aides, etc.

# "OPERATIONAL TASKS"

- Security related work not related to user stories
- Things like patches, scans, significant vulnerabilities
- Extra reviews of risky code
- Often, but not always, goes into the backlog

# TEAM

- Main product dev teams in one place
- Three scrum teams
- Two week sprints
- Testing team
- Ops team
- Architect(s) + support functions
- Client SDK teams "right-shored"
- Full-time security manager -> security architect
- One of the devs was nominated as "security responsible"

# KEY CHALLENGES

- Lots of historical baggage (known issues a.k.a. "technical/security debt")
- High pressure to push out new features
- Also strong focus on availability
- Security on back burner
- Keep security on the table continuously, not ad-hoc

# KEY ACTIVITIES

- Epics, stories, features were complemented with security reviews/discussions
- Architecture was out of band, more forward-looking
- Security manager was changed to a security architect (possible due to attrition)
- Security sprints were conducted to "clear" a lot of old debt
- Sprint backlog items were pre-munched for security aspects (had to have basic definition in place)
- Code scanning, vuln scanning etc. was end of sprint or out of band
- Security audits, pentests, etc. were also out of band
- Testing was both focused unit testing & broader integration testing (added sec cases)

QUESTIONS?