

Von ~~Internetseiten~~ Webseiten zu verteilten Cloud-Anwendungen: Entwicklungen in der Web- Sicherheit.

Thomas Roessler, W3C <tlr@w3.org> @roessler



“Die HTML-Seiten
werden häufig durch
aktive Inhalte wie
Flash und JavaScript
erweitert.”





Join the millions of businesses that have gone Google.

Each day, thousands of companies are going Google by switching to Google Apps – a web-based suite of messaging and collaboration applications. It's all hosted by Google, and designed with security and reliability in mind, saving your company the frustrations and hassles of managing traditional IT solutions yourself. Find out how others have switched from Microsoft® Exchange or Lotus Notes to Google Apps.

[Contact Google](#)

Get an Easy-To-Use Web-Based Contact Manager (CRM)

30 Day Free Trial. 30 Seconds to Sign Up. No Credit Card Required.



BigContacts CRM Will Help You...



Office Web Apps on Facebook [Like](#) 9k

EXTEND YOUR OFFICE EXPERIENCE TO THE WEB

Access, edit, and share your Word,
Excel, PowerPoint and OneNote
documents online from almost
anywhere.

[Get started free](#)



See how—and why—to use Office Web Apps.



HTML5

& friends



transformative,
interoperable
Applikationsplattform
für verteilte
Anwendungen



Netzwerkeffekte im Browser

postMessage

CORS & XHR2

WebRTC

websockets

Web Intents



Web Intents

Dynamische Konstruktion von Mashups



Sensoren
Mikrofon
Kamera
Beschleunigung
Touch



Hangouts with extras

+ Invite

Share screen



Exit

Documents

Notes

Sketchpad

+ Add document

Group Chat

You are now off the record [Learn more](#) [Cancel](#)



No one is here right now.

Why don't you [invite others](#), or
[add a document?](#)

<<

1 participant





[HOME](#)

[SPEAKERS](#)

[SCHEDULE](#)

[VENUE/TRAVEL](#)

[REGISTER NOW](#)

newgame.eventbrite.com

[UNLOCK DISCOUNTS!](#)

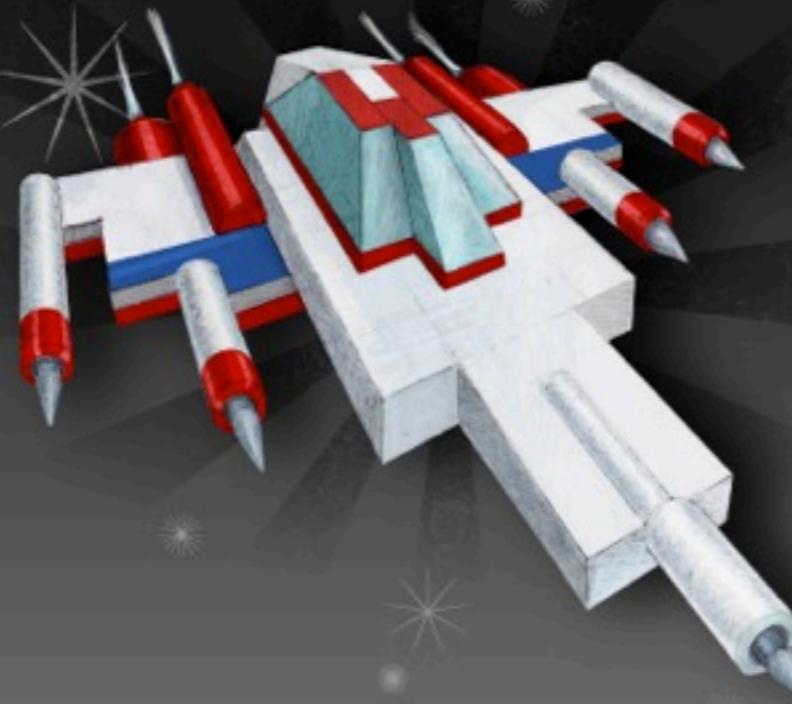
Register today to unlock deals
from our sponsors/partners

Join us at Yerba Buena Center for the Arts for two days with the world's foremost HTML5 game developers and learn how to bring your gaming vision to the web now.

NO TICKETS LEFT

START NEW GAME

0 Days Left



NOV 1-2
SF
SAN FRANCISCO

SOLD OUT!

Blast Off! Play in to HTML5 Games!
Tickets Have SOLD OUT!!



[Like](#)

[Tweet](#)

(Psst! Check out the [New Game coding contest](#) at CoderCharts.)

Game-changing Keynotes from Two Gaming Masterminds:



**RICH
HILLEMAN**

Creative Director, EA



**PAUL
BAKAUS**

CTO, Zynga Germany



Share the New Game Fever!

**DOWNLOAD
WEB BADGES**

For Attendees/Speakers



Transformationen



statisch
interaktiv



~~Verbraucher~~ Enterprise





Join the millions of businesses that have gone Google.

Each day, thousands of companies are going Google by switching to Google Apps – a web-based suite of messaging and collaboration applications. It's all hosted by Google, and designed with security and reliability in mind, saving your company the frustrations and hassles of managing traditional IT solutions yourself. Find out how others have switched from Microsoft® Exchange or Lotus Notes to Google Apps.

[Contact Google](#)

Get an Easy-To-Use Web-Based Contact Manager (CRM)

30 Day Free Trial. 30 Seconds to Sign Up. No Credit Card Required.



BigContacts CRM Will Help You...

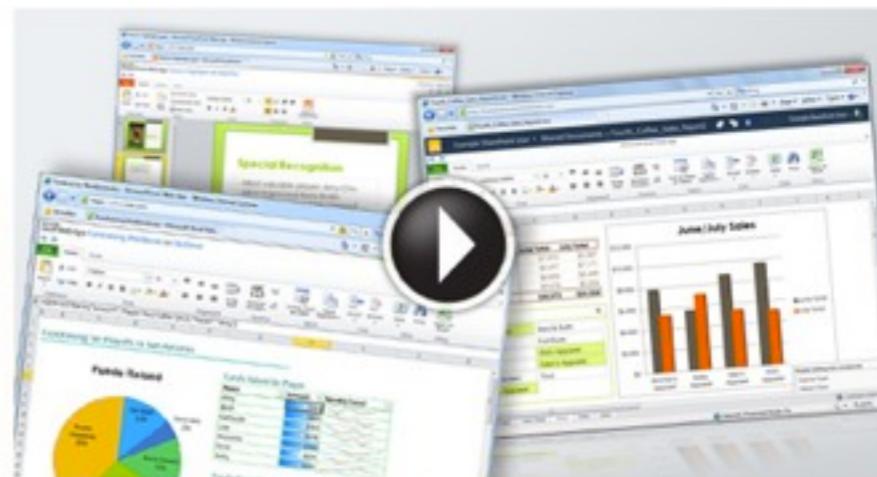


Office Web Apps on Facebook [Like](#) 9k

EXTEND YOUR OFFICE EXPERIENCE TO THE WEB

Access, edit, and share your Word,
Excel, PowerPoint and OneNote
documents online from almost
anywhere.

[Get started free](#)



See how—and why—to use Office Web Apps.



Google Apps Customer Explains How Microsoft Tried To Change His Mind

Matt Rosoff | Nov. 14, 2011, 5:41 PM | 🔥 2,238 | 🗣 3

[f Recommend](#)

5

[in Share](#)

15

[Tweet](#)

47

[+1](#)

13

[Email](#)

AAA

A couple years ago, we heard a rumor that Microsoft viewed Google Apps as the number-one threat to its enterprise business.

Apparently, whenever a big Microsoft customer announced a plan to use Gmail or Google Apps, Microsoft would sic a special team on them to try and change their mind.

Now, we know it's true.

Michael Rodger is the IT director of a Canadian hotel chain called Delta Hotels. In 2009, they decided to move their company's email to the cloud.



He can be very persuasive in person.



Schutzziel
**Daten und
Anwendungen
in der Cloud**

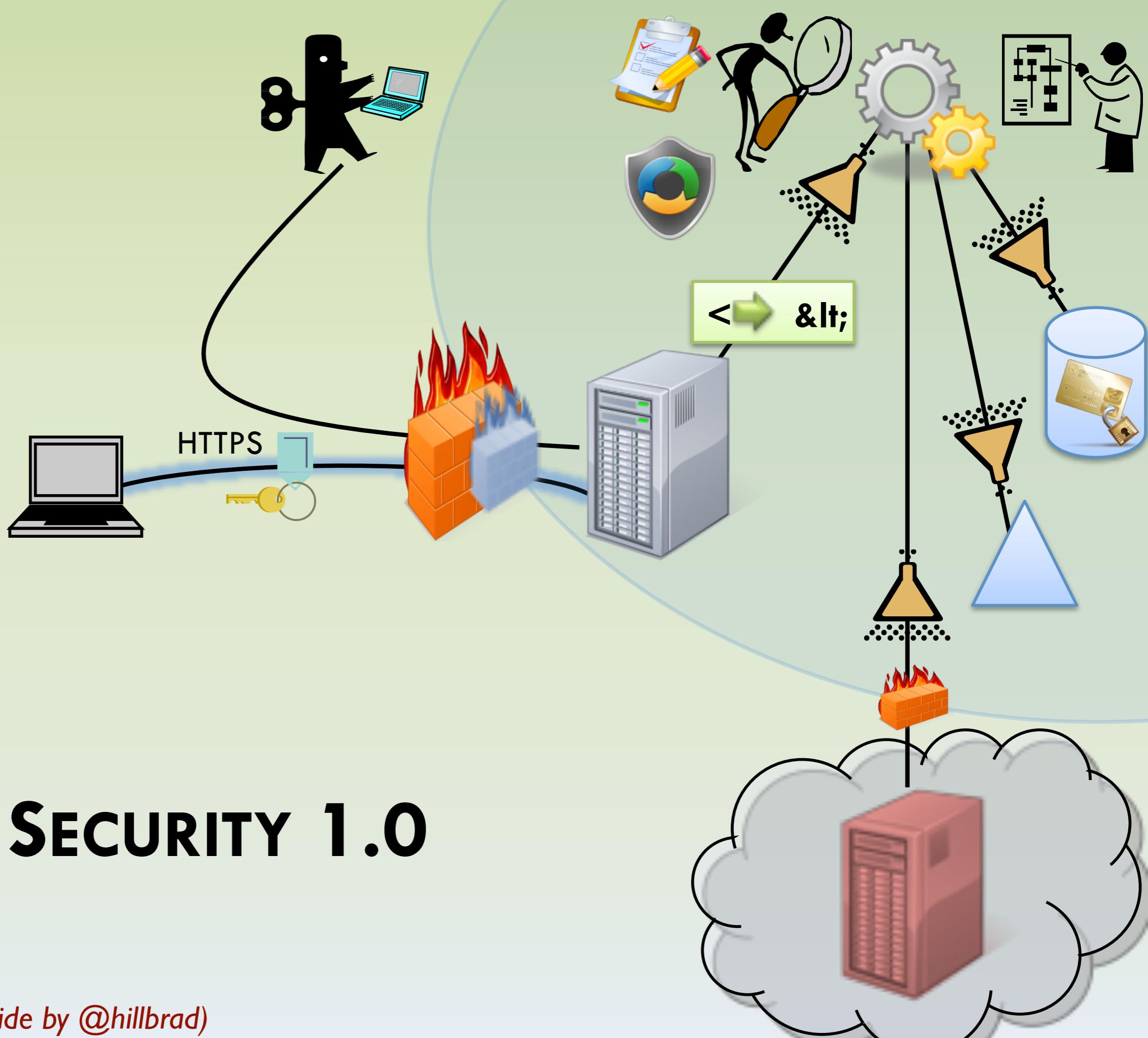


“Die HTML-Seiten
werden häufig durch
aktive Inhalte wie
Flash und JavaScript
erweitert.”



**Server-Sicherheit
Malware-Schutz
Netzwerksicherheit
OWASP Top 10**



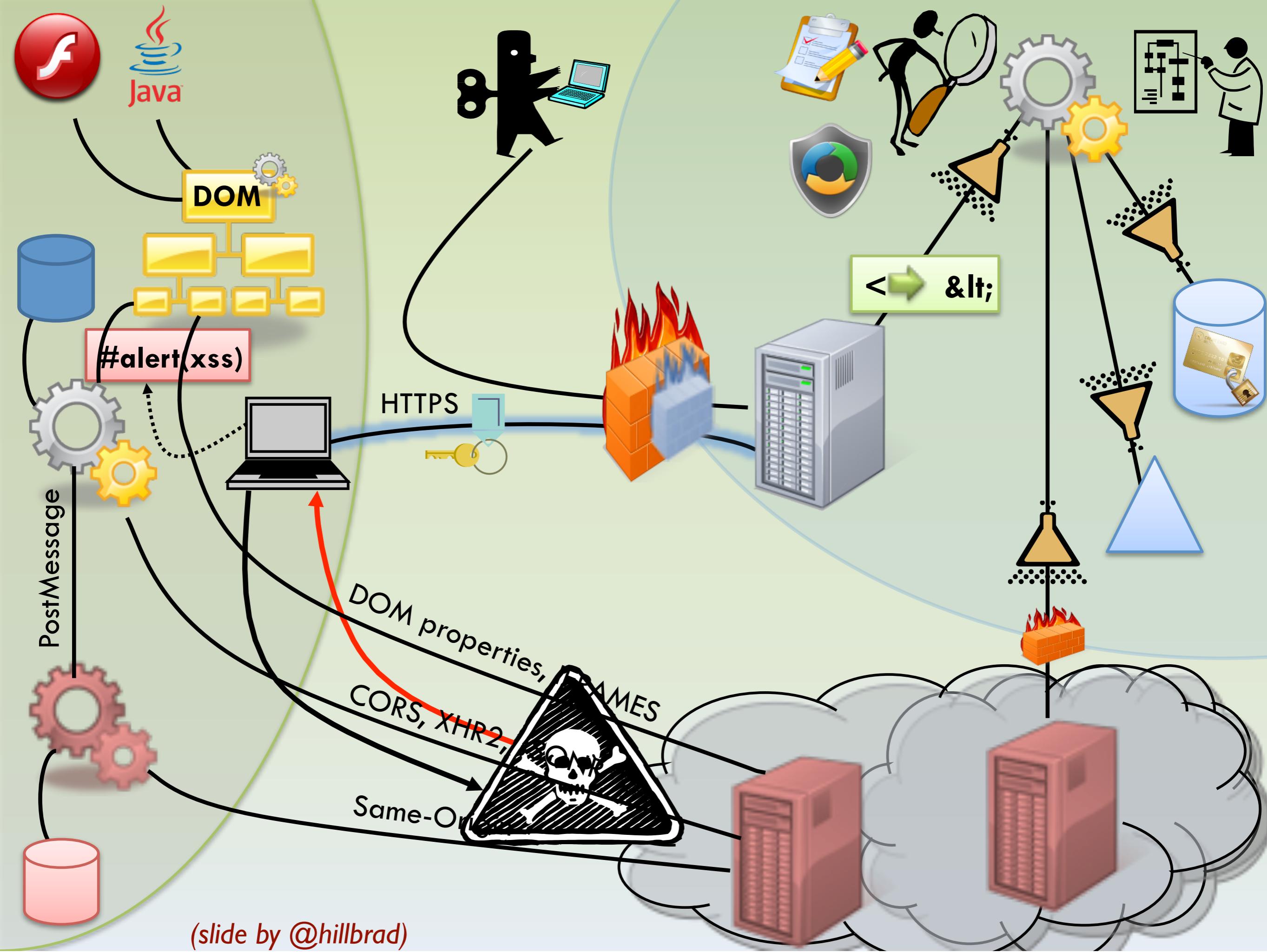


WEB SECURITY 1.0

(slide by @hillbrad)

~~client/server~~
verteilte
Anwendungen





~~Server-Sicherheit~~

~~Malware-Schutz~~

~~Netzwerksicherheit~~

~~OWASP Top 10~~

Webapp-Sicherheit



Verteidigung im Client
**Datenströme im
Browser**
Serverlose Apps



**Codeinjektion wird im
Client ausgeführt**



Some stats about DOM XSS

We downloaded top Alexa 1 million sites and analyzed the first 100 in order to verify the presence of **exploitable** DOM Based Cross Site Scripting vulnerabilities.

Using DOMinator we found that **56 out of 100** (56% of sites) were vulnerable to reliable DOMXss attacks.

Some analysis example can be found [here](#) and [here](#).

We'll release a white paper about this research, in the meantime you can try to reach our results using DOMinator.

<http://blog.mindedsecurity.com/2011/05/dominator-project.html>



Kooperative Durchsetzung von Sicherheitspolicies



CSP

Content Security Policy



zum Beispiel
inline <script>
eval &c
data: . . .



Content Security Policy

Unofficial Draft 15 November 2011

Editors:

[Brandon Sterne, Mozilla Corporation](#)
[Adam Barth, Google, Inc.](#)

This document is licensed under a [Creative Commons Attribution 3.0 License](#).

Abstract

This document defines a policy language used to declare a set of content restrictions for a web resource, and a mechanism for transmitting the policy from a server to a client where the policy is enforced.

Status of This Document

This document is merely a public working draft of a potential specification. It has no official standing of any kind and does not represent the support or consensus of any standards organisation.

Table of Contents

- 1. Introduction
- 2. Conformance Criteria
 - 2.1 Terminology
- 3. Syntax
 - 3.1 Policy Delivery
 - 3.1.1 `X-Content-Security-Policy` Response Header
 - 3.1.2 `<meta http-equiv="X-Content-Security-Policy">` HTML Element



Grenzen zwischen Applikationen



Google Chrome, Firefox Adding 'Do Not Track' Tools

H http://www.huffingtonpost.com/2011/01/2 Google

Google Chrome, Firefox Adding 'D...

BIG NEWS: Internet | Twitter | NASA | Cyber Security | Energy Debates | More...

LOG IN | SIGN UP

FEBRUARY 7, 2011

THE HUFFINGTON POST

FIND EXACTLY WHAT YOU'RE LOOKING FOR WITH BING.

bing Dorset, England Microsoft

FRONT PAGE | POLITICS | BUSINESS | MEDIA | ENTERTAINMENT | COMEDY | SPORTS | STYLE | WORLD | GREEN | FOOD | TRAVEL | TECH

LIVING | HEALTH | DIVORCE | ARTS | BOOKS | RELIGION | IMPACT | EDUCATION | COLLEGE | NY | LA | CHICAGO | DENVER | BLOGS

White iPhone 4 Shelf Space Spotted

U.S. Has Secret Tools To Force Internet On Dictators

Sprint SEE WHAT Sprint HAS UP ITS SLEEVE

Sprint To Unveil Tablet-Like Phone?

Google Chrome, Firefox Adding 'Do Not Track' Tools

DANA WOLLMAN | 01/24/11 05:20 PM | AP

Inspiring Funny Obsolete Scary Must-Have Amazing Innovative Nerdy

Read More: Chrome Do Not Track, Firefox Do Not Track, Firefox Tracking, Google Chrome, Google Chrome Do Not Track, Google Chrome OS, Technology News

SHARE THIS STORY

Like Sign Up to see what your friends like.

14 39 3 13

f share t tweet e email c comment

NEW YORK — The Firefox and Google Chrome browsers are getting tools to help users block advertisers from collecting information about them. ... Fowler, a technology and privacy officer for Firefox maker Mozilla, said the "Do Not Track" tool will be the first in a series of steps designed to guard privacy. He didn't say when the tool will be available.

Google Chrome users can now download a browser plug-in that blocks advertisers – but only from ad networks that already let people decline personalized, targeted ads. According to Google Inc., these include the top 15 advertising networks, as rated by the research group comScore, a group that includes AOL Inc., Yahoo Inc. and Google itself.

EARN THE TRUTH BOUT "GASLAND" CLICK HERE

anga

FOLLOW HUFFINGTON POST

f t a n b e r

MOST POPULAR ON HUFFPOST 1 of 2

WATCH: Christina Aguilera Totally Messes Up National

<script src="...">



JSONP



Strukturierte Kommunikation zwischen Applikationen





Cross-Origin Resource Sharing

W3C Working Draft 27 July 2010

This Version:

<http://www.w3.org/TR/2010/WD-cors-20100727/>

Latest Version:

<http://www.w3.org/TR/cors/>

Latest Editor Draft:

<http://dev.w3.org/2006/waf/access-control/>

Previous Versions:

<http://www.w3.org/TR/2009/WD-cors-20090317/>

<http://www.w3.org/TR/2008/WD-access-control-20080912/>

<http://www.w3.org/TR/2008/WD-access-control-20080214/>

<http://www.w3.org/TR/2007/WD-access-control-20071126/>

<http://www.w3.org/TR/2007/WD-access-control-20071001/>

<http://www.w3.org/TR/2007/WD-access-control-20070618/>

<http://www.w3.org/TR/2007/WD-access-control-20070215/>

<http://www.w3.org/TR/2006/WD-access-control-20060517/>

<http://www.w3.org/TR/2005/NOTE-access-control-20050613/>

Editor:

[Anne van Kesteren \(Opera Software ASA\)](#) <annevk@opera.com>

Copyright © 2008 W3C® ([MIT](#), [ERCIM](#), [Keio](#)), All Rights Reserved. W3C [liability](#), [trademark](#) and [document use rules apply](#).



<iframe>



WARNING: Facebook Clickjacking Attack Spreading Through “Likes”



May 31, 2010 by Christina Warren

333

Like

Send

16885 likes. [Sign Up](#) to see what your friends like.

A new clickjacking worm is spreading through Facebook via the “Like” feature. The attack, which is said to have hit hundreds of thousands of users, uses a combination of social engineering and clickjacking to make it appear as if a user has “liked” a link.

The messages that are being used in the link text include, “LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE,” “This man takes a picture of himself EVERYDAY for 8 YEARS!!,” “The Prom Dress That Got This Girl Suspended From School” and “This Girl Has An Interesting Way Of Eating A Banana, Check It Out!”



**x-frame-options
ist keine Lösung**



W3C Web Application Security Working Group



Kommunikation zwischen Webapps

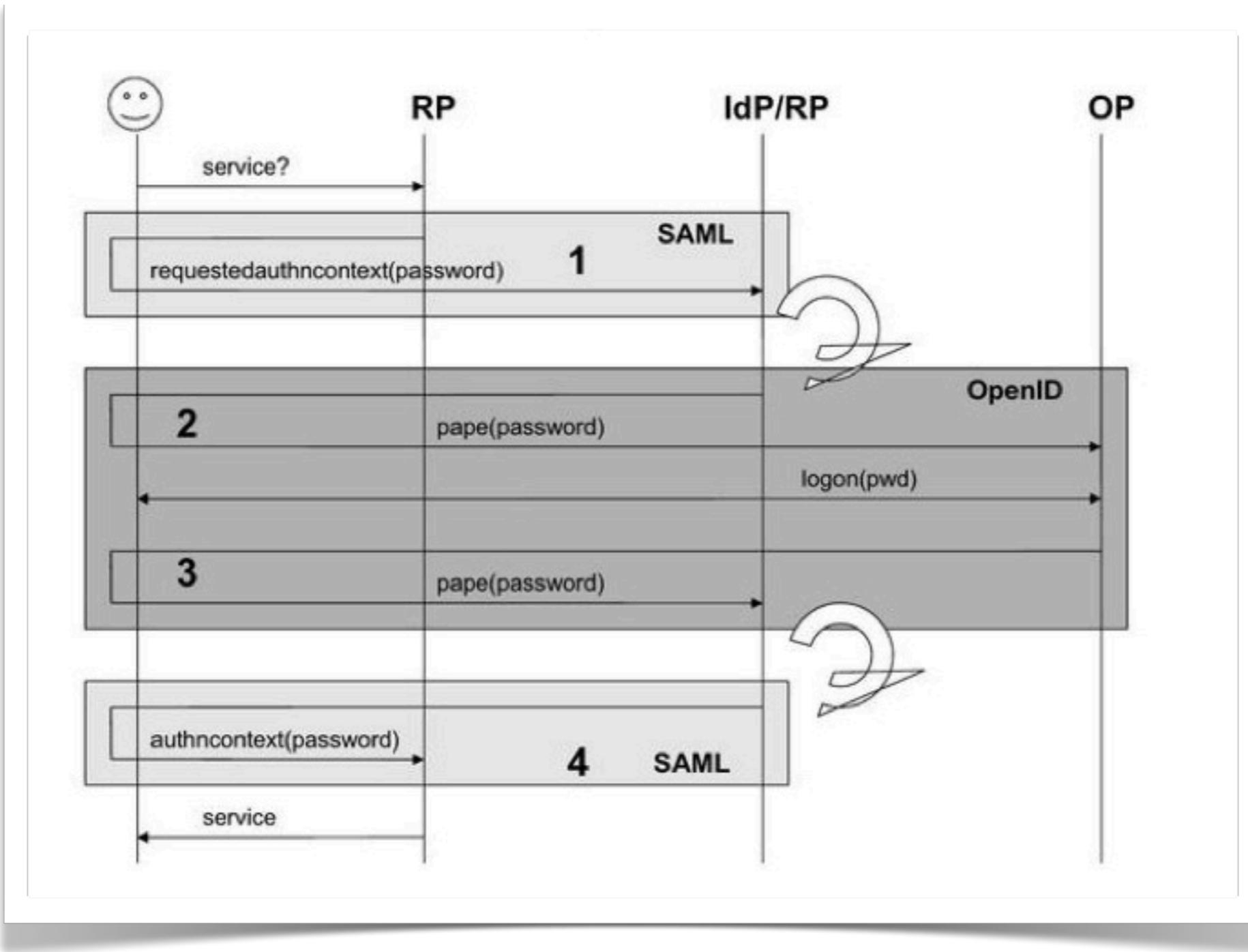


CORS
postMessage
Web Intents
WebRTC



Protokolle zwischen
Webapplikationen,
z.B.
Identitätsmanagement







<http://www.flickr.com/photos/compujera/47025604/>

W3C Workshop on Identity in the Browser

24/25th May 2011, Mountain View (USA)

[About W3C](#) [Report](#) [Call for Participation](#) [Papers](#) [Agenda](#) [Nearby Events](#) [Venue](#)

Call For Participation

Background

Now available:
[Final Report](#)

As the Web becomes increasingly a focal point for economic and social activity, there is an urgent need for trustworthy, widely-applicable digital identity management. This includes the need for authentication and authorization to work across multiple web-sites, enterprises, devices, and browsers in a uniform and easy-to-use manner. For critical enterprise activity, effective government engagement, and sensitive social information accessed over the Web, a higher level of identity assurance, privacy protection, and security is required beyond simple username/password combinations. To address many of these issues, digital identity should become a core part of Web architecture, enabled by a combination of server and client-side solutions. Achieving this vision, however, requires addressing numerous technical, operational, policy, and legal issues. This



Hosted by Mozilla
in Mountain View (USA)

Workshop sponsors:



The Security Division of EMC



BrowserID is an easier way to sign in

A graphic showing a blue 'Sign in' button with a person icon and an arrow pointing right, set against a light gray background.

Sign in

- 1 On your favorite website that supports BrowserID,
Click the 'Sign In' button

Sign in using

home@example.com

work@example.com

- 2 Select your preferred Email



2. Identify the User

Instead of displaying a form on your site which takes a *username* and *password*, use the BrowserID JavaScript API when the user clicks your sign-in button:

```
navigator.id.getVerifiedEmail(function(assertion) {  
  if (assertion) {  
    // This code will be invoked once the user has successfully  
    // selected an email address they control to sign in with.  
  } else {  
    // something went wrong! the user isn't logged in.  
  }  
});
```

Upon a successful sign-in, you'll be called back with an `assertion`, a string containing a signed claim that proves the user is who they say they are.



**Komplexere
Sicherheitsprotokolle
zwischen Webapps?**



```
01. [Supplemental]
02. interface Crypto {
03.   readonly attribute CryptoPk pk;
04.   readonly attribute CryptoSign sign;
05. };
06.
07. [Constructor(in DOMString algorithm)]
08. interface CryptoHash {
09.   void append(in ArrayBuffer data);
10.   ArrayBuffer finish();
11. };
12.
13. [Constructor(in DOMString algorithm, in ArrayBuffer key)]
14. interface CryptoHmac {
15.   void append(in ArrayBuffer data);
16.   ArrayBuffer finish();
17. };
18.
19. [Callback=FunctionOnly, NoInterfaceObject] interface
20. ↗ GenerateKeypairCallback {
21.   void onsuccess(ArrayBuffer keyID, ArrayBuffer pubKey);
22. };
23.
24. [Callback=FunctionOnly, NoInterfaceObject] interface
25. ↗ GetPublicKeyCallback {
26.   void onsuccess(ArrayBuffer publicKey);
27. };
28.
29. [Callback=FunctionOnly, NoInterfaceObject] interface PKEncryptCallback {
30.   void onsuccess(ArrayBuffer message);
31. };
```



coming soon

Kryptographische APIs für JavaScript Identity-APIs im Browser



HTML5

& friends





Join the millions of businesses that have gone Google.

Each day, thousands of companies are going Google by switching to Google Apps – a web-based suite of messaging and collaboration applications. It's all hosted by Google, and designed with security and reliability in mind, saving your company the frustrations and hassles of managing traditional IT solutions yourself. Find out how others have switched from Microsoft® Exchange or Lotus Notes to Google Apps.

[Contact Google](#)

Get an Easy-To-Use Web-Based Contact Manager (CRM)

30 Day Free Trial. 30 Seconds to Sign Up. No Credit Card Required.

BigContacts CRM Will Help You...



Starting As Low As:
\$15⁰⁰
Per Month

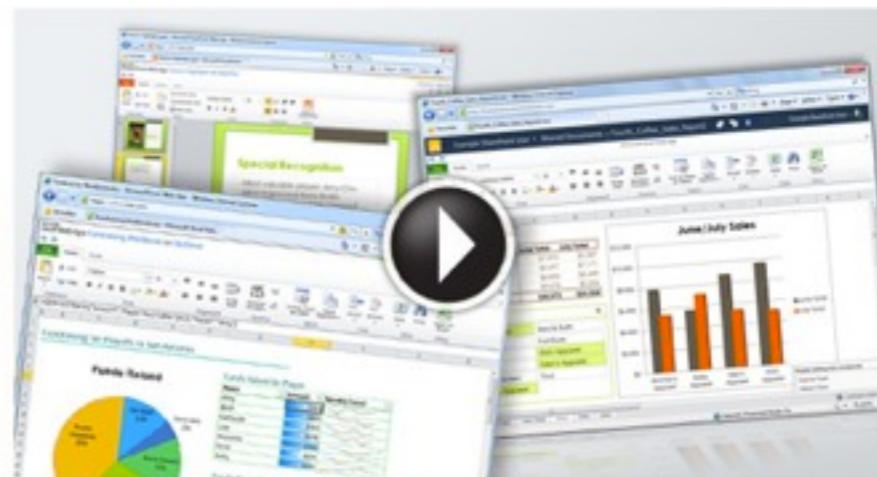


Office Web Apps on Facebook [Like](#) 9k

EXTEND YOUR OFFICE EXPERIENCE TO THE WEB

Access, edit, and share your Word,
Excel, PowerPoint and OneNote
documents online from almost
anywhere.

[Get started free](#)



See how—and why—to use Office Web Apps.



Google Apps Customer Explains How Microsoft Tried To Change His Mind

Matt Rosoff | Nov. 14, 2011, 5:41 PM | 🔥 2,238 | 🗣 3

[f Recommend](#)

5

[in Share](#)

15

[Tweet](#)

47

[+1](#)

13

[Email](#)

AAA

A couple years ago, we heard a rumor that Microsoft viewed Google Apps as the number-one threat to its enterprise business.

Apparently, whenever a big Microsoft customer announced a plan to use Gmail or Google Apps, Microsoft would sic a special team on them to try and change their mind.

Now, we know it's true.

Michael Rodger is the IT director of a Canadian hotel chain called Delta Hotels. In 2009, they decided to move their company's email to the cloud.



He can be very persuasive in person.



