HTML5 Web Security

Michael Schmidt – IT Security Analyst
michael.schmidt@csnc.ch

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What's this talk about?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

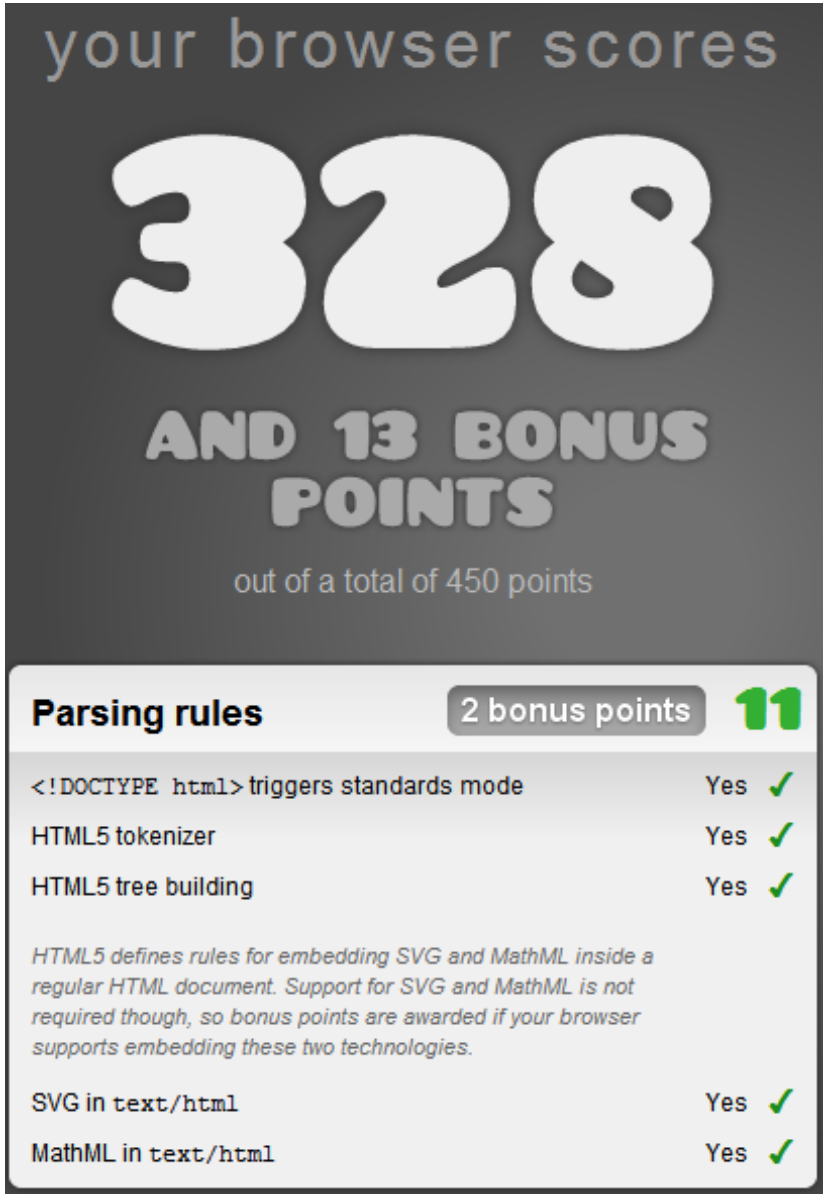
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

What is HTML5?

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

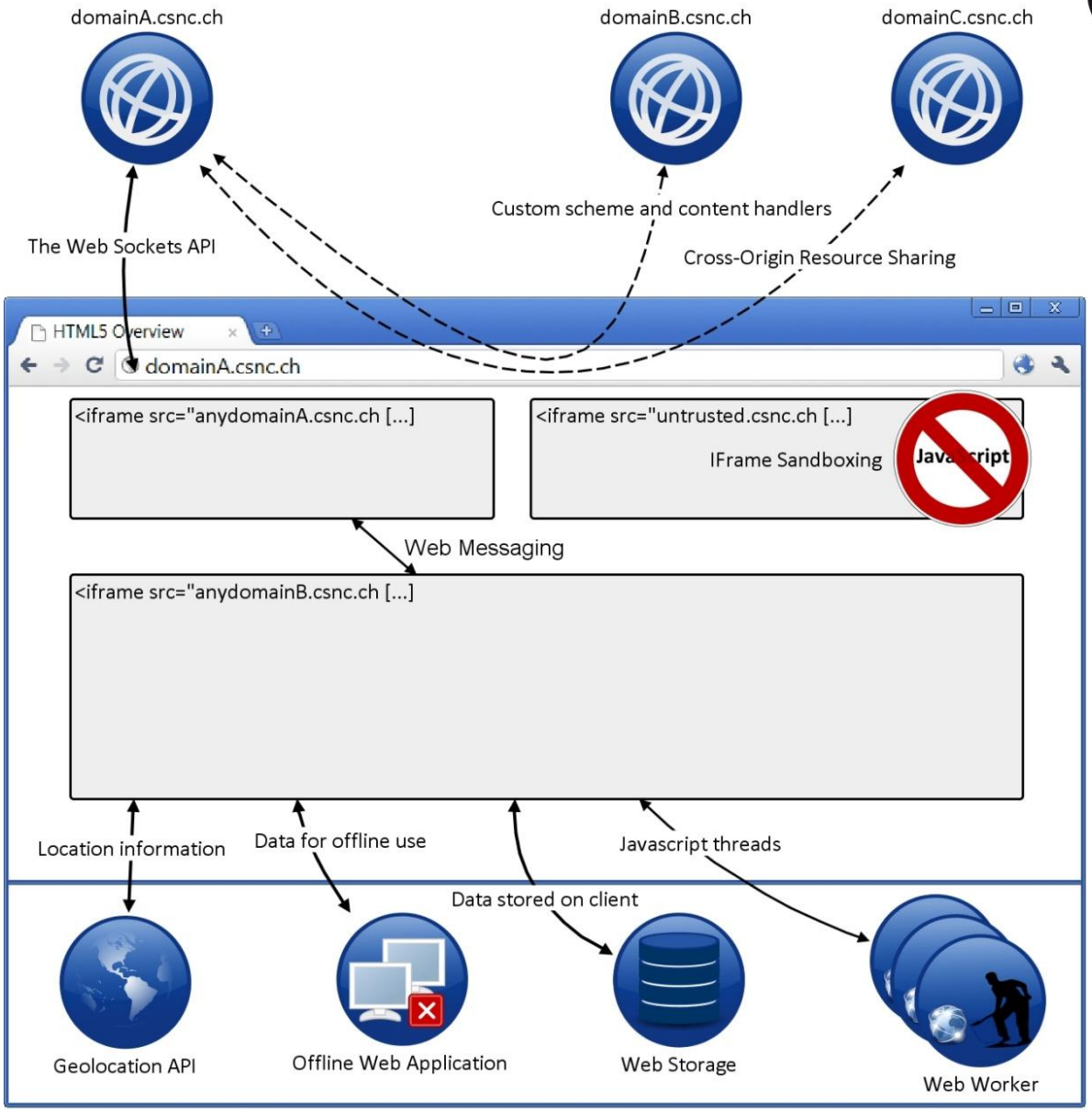
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

HTML5 TEST - http://html5test.com/



out of a total of 450 points

Overview

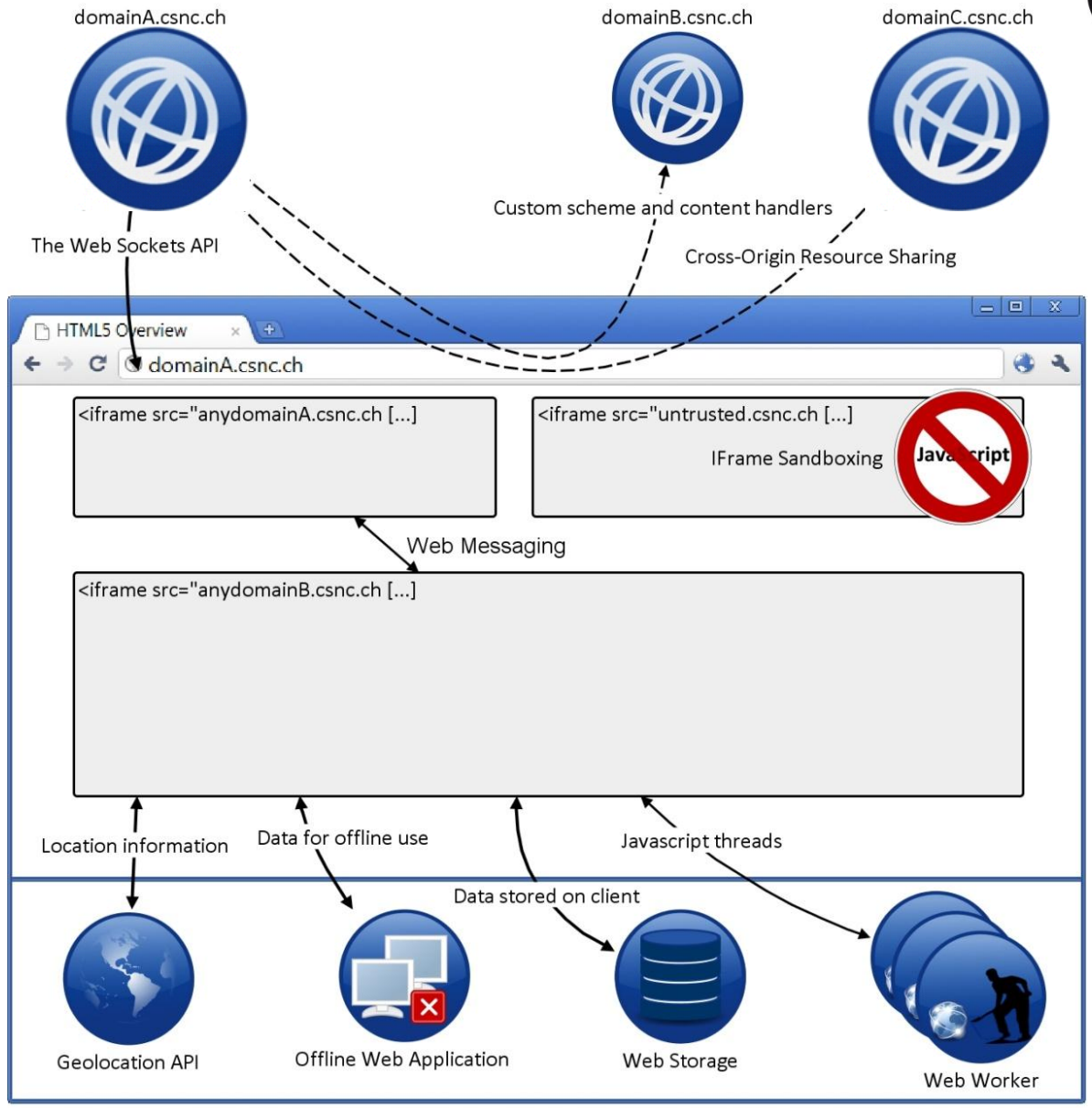

domainA.csnc.ch
domainB.csnc.ch
domainC.csnc.ch
The Web Sockets API
Custom scheme and content handlers
Cross-Origin Resource Sharing
HTML5 Overview
domainA.csnc.ch
<iframe src="anydomainA.csnc.ch [...]
<iframe src="untrusted.csnc.ch [...]
IFrame Sandboxing
Web Messaging
<iframe src="anydomainB.csnc.ch [...]
Location information
Data for offline use
Data stored on client
Javascript threads
Geolocation API
Offline Web Application
Web Storage
Web Worker

Vulnerabilities, Threats and Countermeasures (if any)

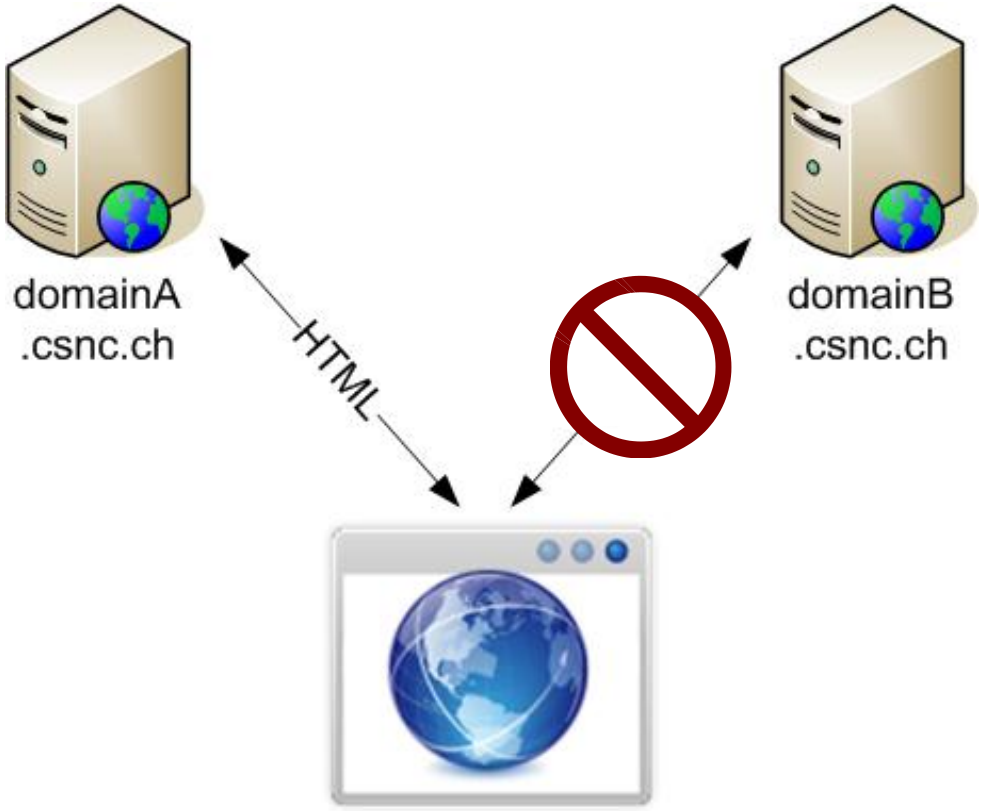
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

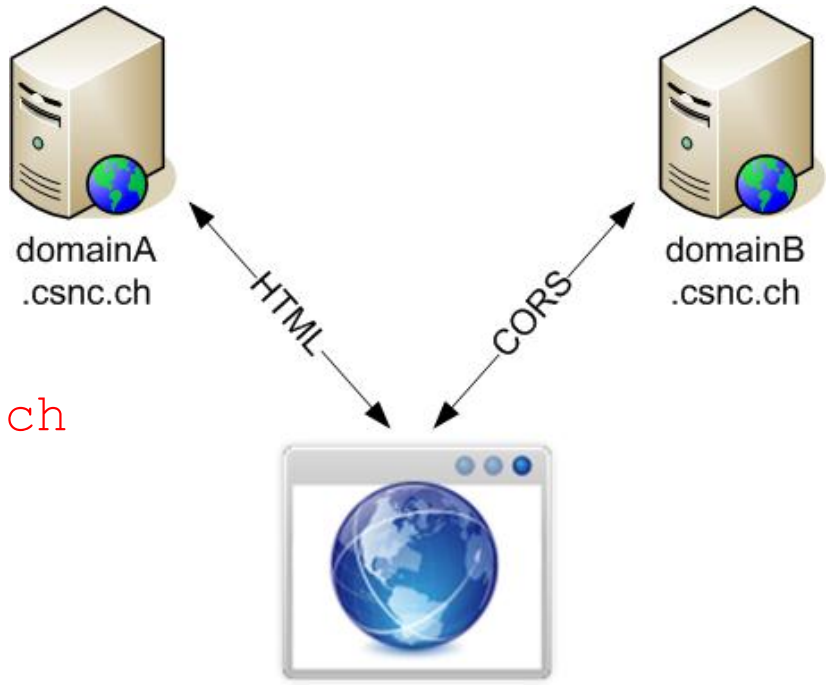
Cross-Origin Resource Sharing



Cross-Origin Resource Sharing I

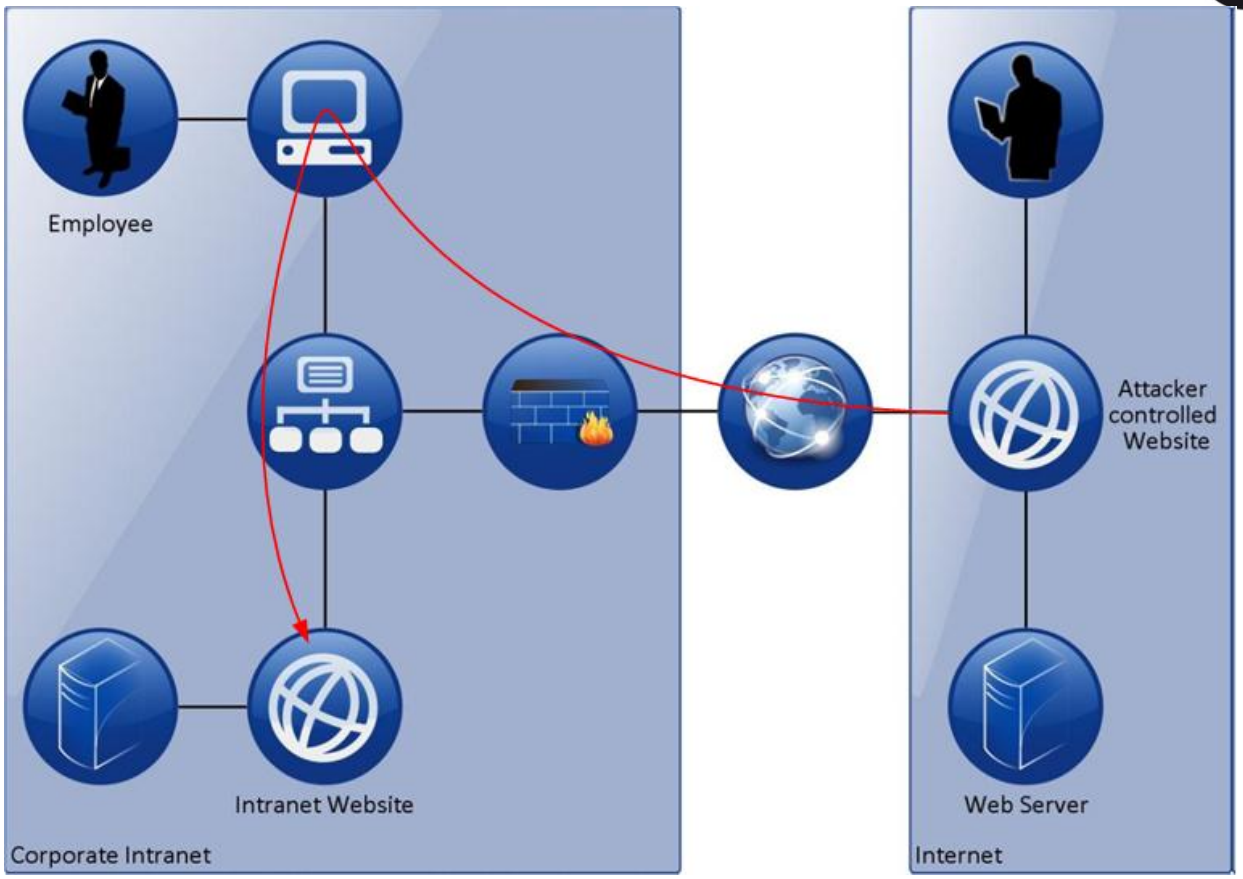


Cross-Origin Resource Sharing II



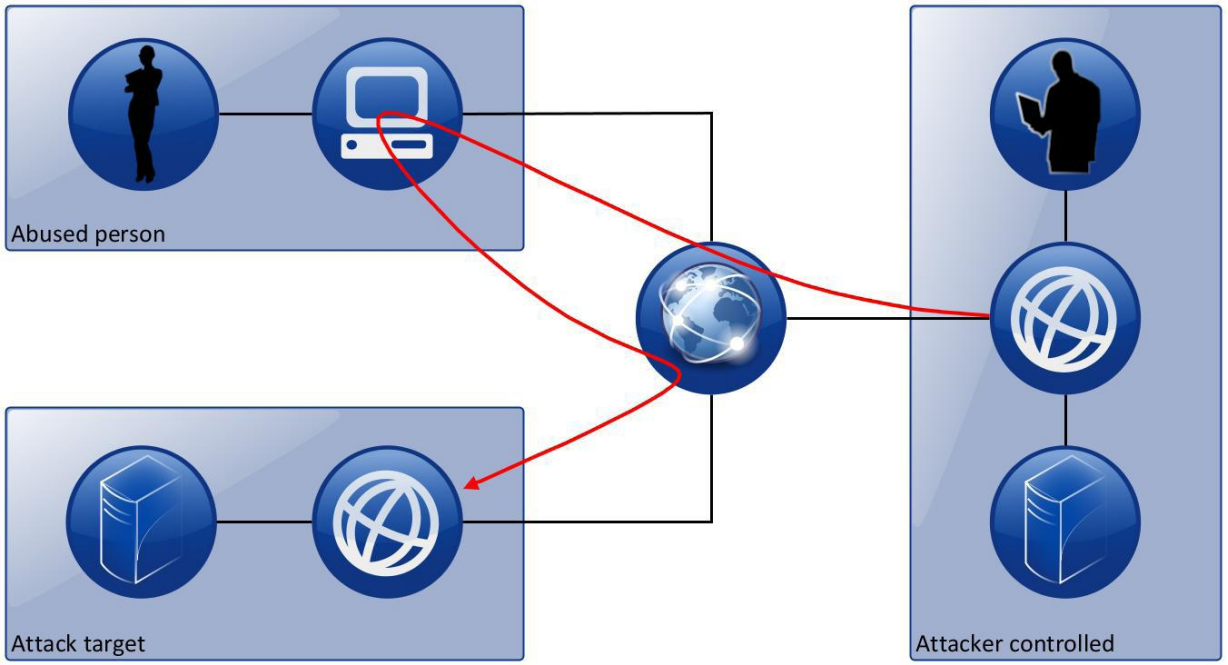

```
GET / HTTP/1.1
Host: domainB.csnc.ch
Origin: http://domainA.csnc.ch


HTTP/1.1 200 OK
Content-Type: text/html
Access-Control-Allow-Origin: http://domainA.csnc.ch
```

CORS – Vulnerabilities & Threats I



- Accessing internal websites
- Scanning the internal network

CORS – Vulnerabilities & Threats II



- Remote attacking a web server
- Easier exploiting of Cross-Site Request Forgery (XSRF)
- Establishing a remote shell *(DEMO)*

Countermeasures

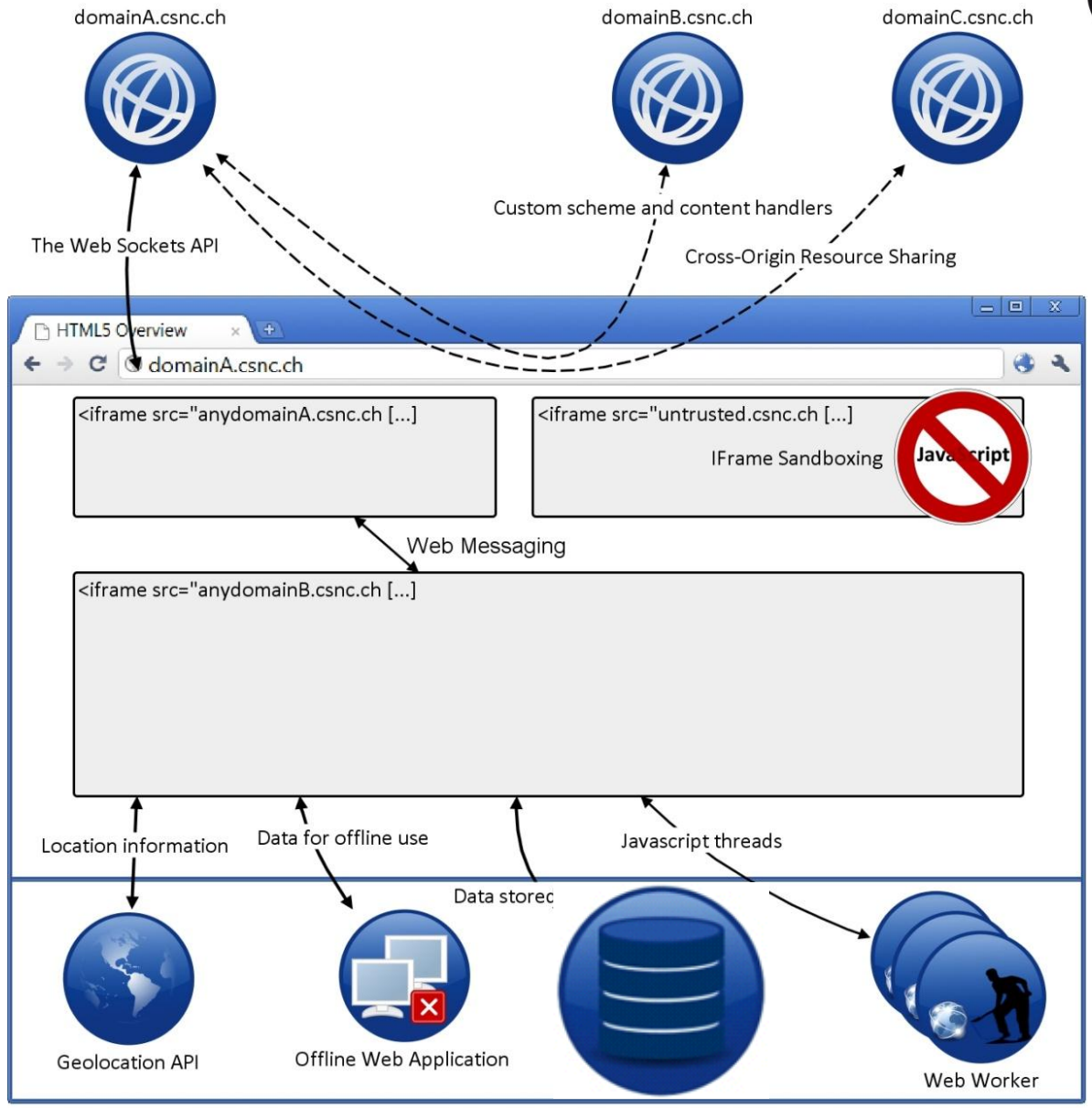
Use the *Access-Control-Allow-Origin* header to restrict the allowed domains.

Never set the header to *.

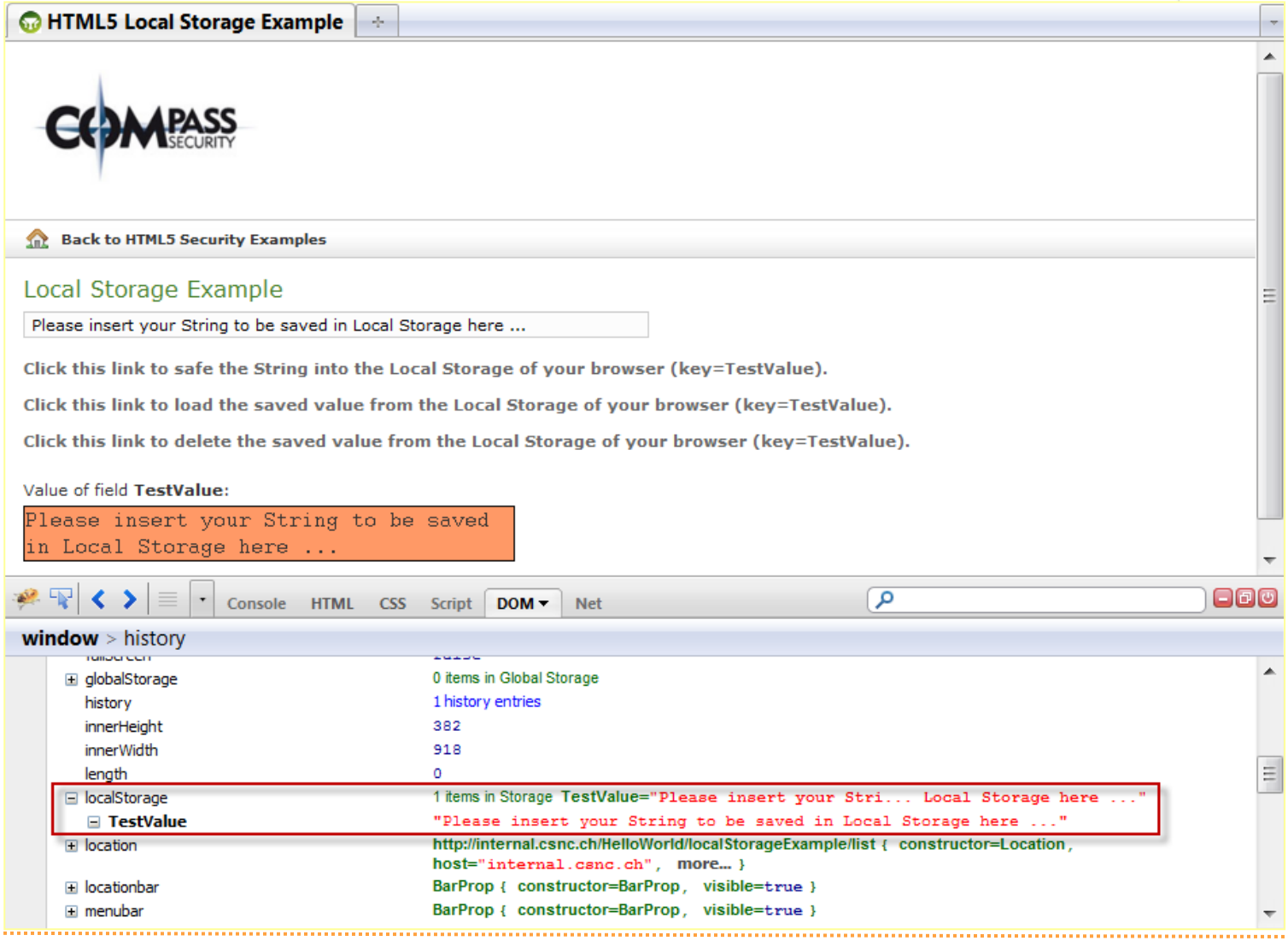
Do not base access control on the origin header.

To mitigate DDoS attacks the Web Application Firewall (WAF) needs to block CORS requests if they arrive in a high frequency.

Web Storage


domainA.csnc.ch
domainB.csnc.ch
domainC.csnc.ch
The Web Sockets API
Custom scheme and content handlers
Cross-Origin Resource Sharing
HTML5 Overview
domainA.csnc.ch
<iframe src="anydomainA.csnc.ch [...]
<iframe src="untrusted.csnc.ch [...]
IFrame Sandboxing
Web Messaging
<iframe src="anydomainB.csnc.ch [...]
Location information
Data for offline use
Data stored
Javascript threads
Geolocation API
Offline Web Application
Web Worker

Web Storage


HTML5 Local Storage Example
Back to HTML5 Security Examples
Local Storage Example
Please insert your String to be saved in Local Storage here ...
Click this link to safe the String into the Local Storage of your browser (key=TestValue).
Click this link to load the saved value from the Local Storage of your browser (key=TestValue).
Click this link to delete the saved value from the Local Storage of your browser (key=TestValue).
Value of field TestValue:
Please insert your String to be saved in Local Storage here ...
Console
HTML
CSS
Script
DOM
Net
window > history
globalStorage
0 items in Global Storage
history
1 history entries
innerHeight
382
innerWidth
918
length
0
localStorage
1 items in Storage TestValue="Please insert your Stri... Local Storage here ..."
TestValue
"Please insert your String to be saved in Local Storage here ..."
location
http://internal.csnc.ch/HelloWorld/localStorageExample/list { constructor=Location, host="internal.csnc.ch", more... }
locationbar
BarProp { constructor=BarProp, visible=true }
menubar
BarProp { constructor=BarProp, visible=true }

Web Storage – Vuln. & Threats

Session Hijacking

- If session identifier is stored in local storage, it can be stolen with JavaScript.
- No *HTTPOnly* flag.

Disclosure of Confidential Data

- If sensitive data is stored in the local storage, it can be stolen with JavaScript.

User Tracking

- Additional possibility to identify a user.

Persistent attack vectors

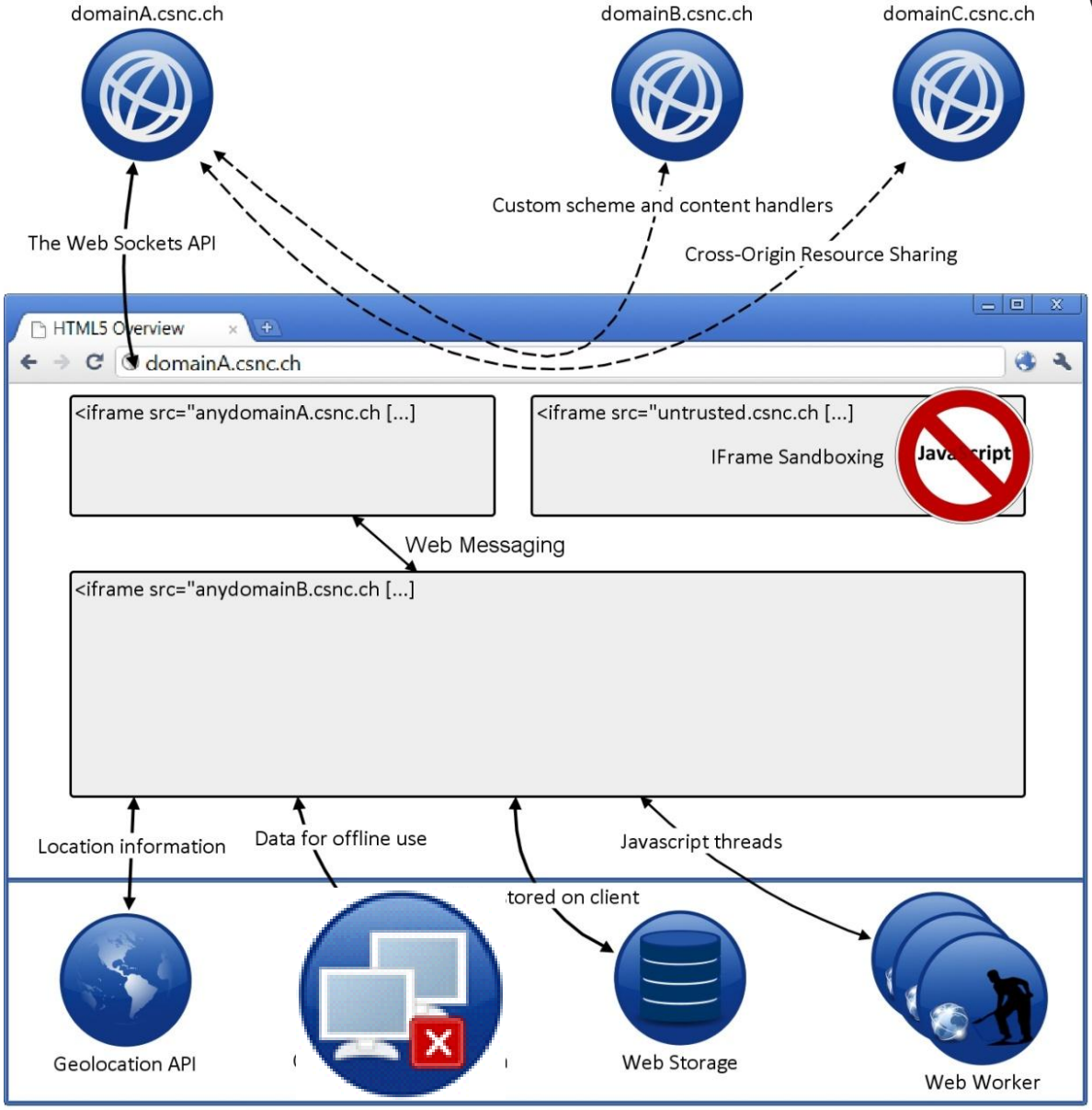
- Attack vectors can be stored persistently in the victim's browser.

Countermeasures

Use cookies instead of Local Storage for session handling.

Do not store sensitive data in Local Storage.

Offline Web Application



Offline Web Application

```
<!DOCTYPE HTML>
<html manifest="/cache.manifest">
<body>
...
```

Example cache.manifest

```
CACHE MANIFEST
/style.css
/helper.js
/csnc-logo.jpg
NETWORK:
/visitor_counter.jsp
FALLBACK:
/ /offline_Error_Message.html
```

OWA – Vulnerabilities & Threats

Cache Poisoning

- Caching of the root directory possible.
- HTTP and HTTPs caching possible.

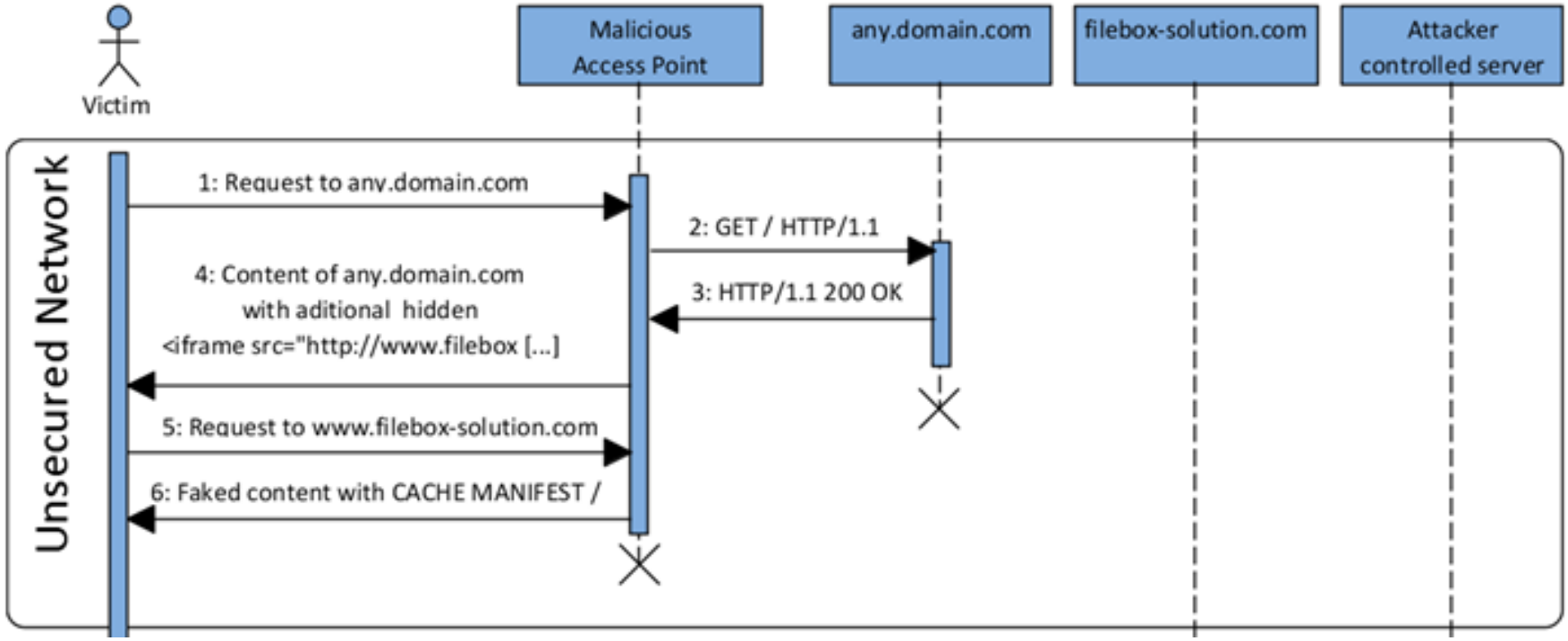
Persistent attack vectors

- Attack vectors can be stored persistently in the victim's browser.

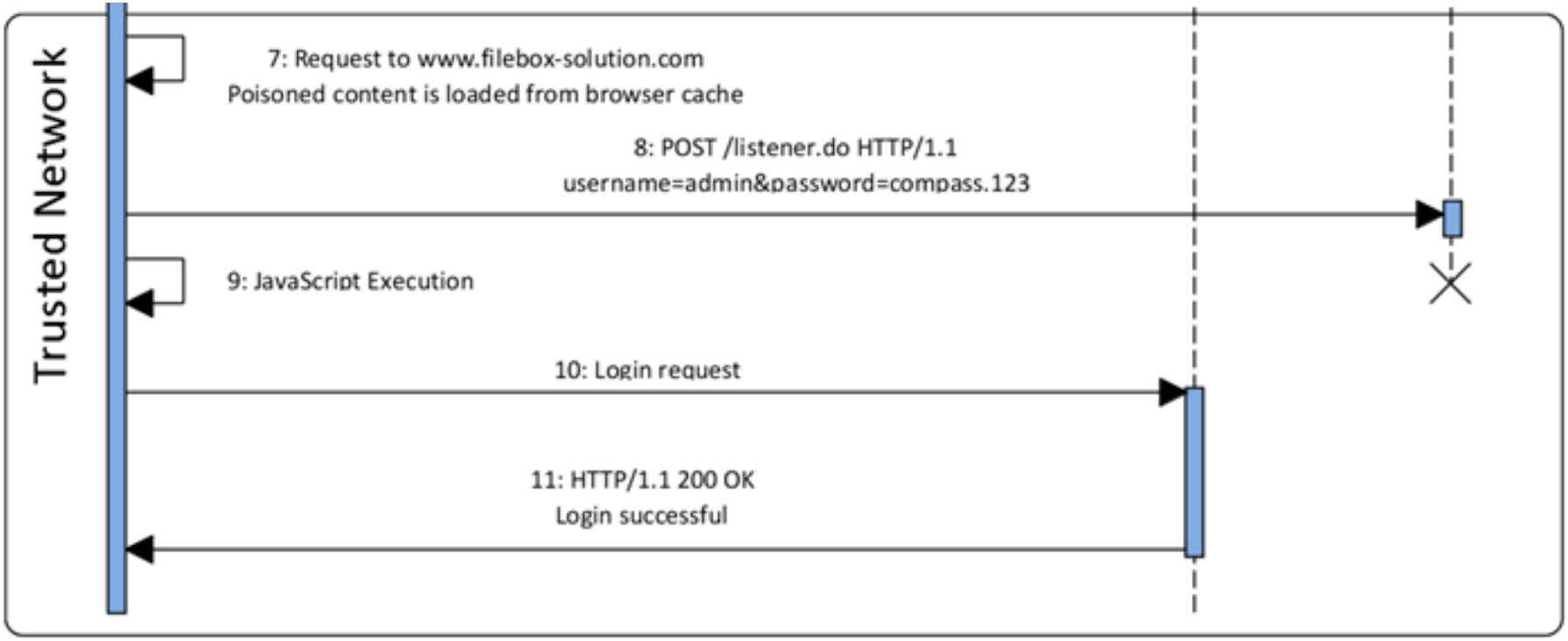
User Tracking

- Additional possibility to identify a user.
- Unique identifiers could be stored along with the cached files.

Offline Web Application – Attack 1/2

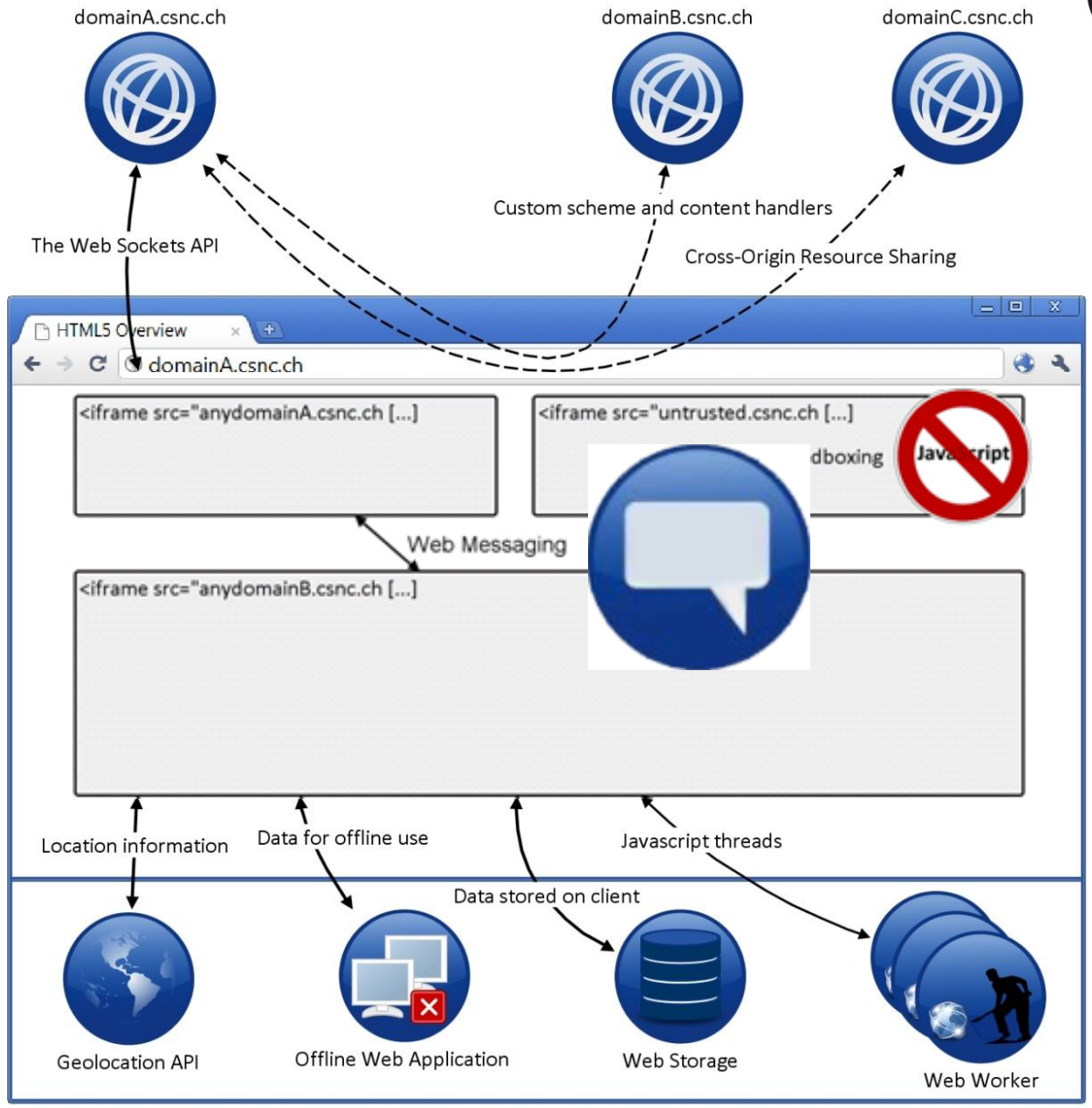


Offline Web Application – Attack 2/2

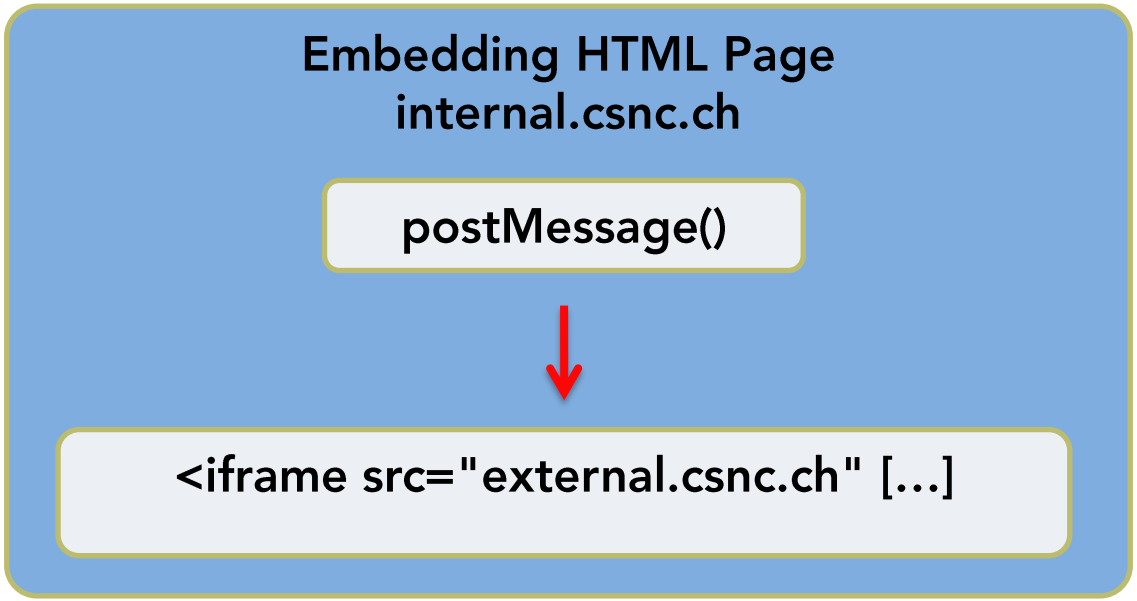


User-Training

Web Messaging



Web Messaging



Stealing confidential data

- Sensitive data may be sent accidently to a malicious Iframe.

Expands attack surface to the client

- Iframes can send malicious content to other Iframes.
- Input validation on the server is not longer sufficient.

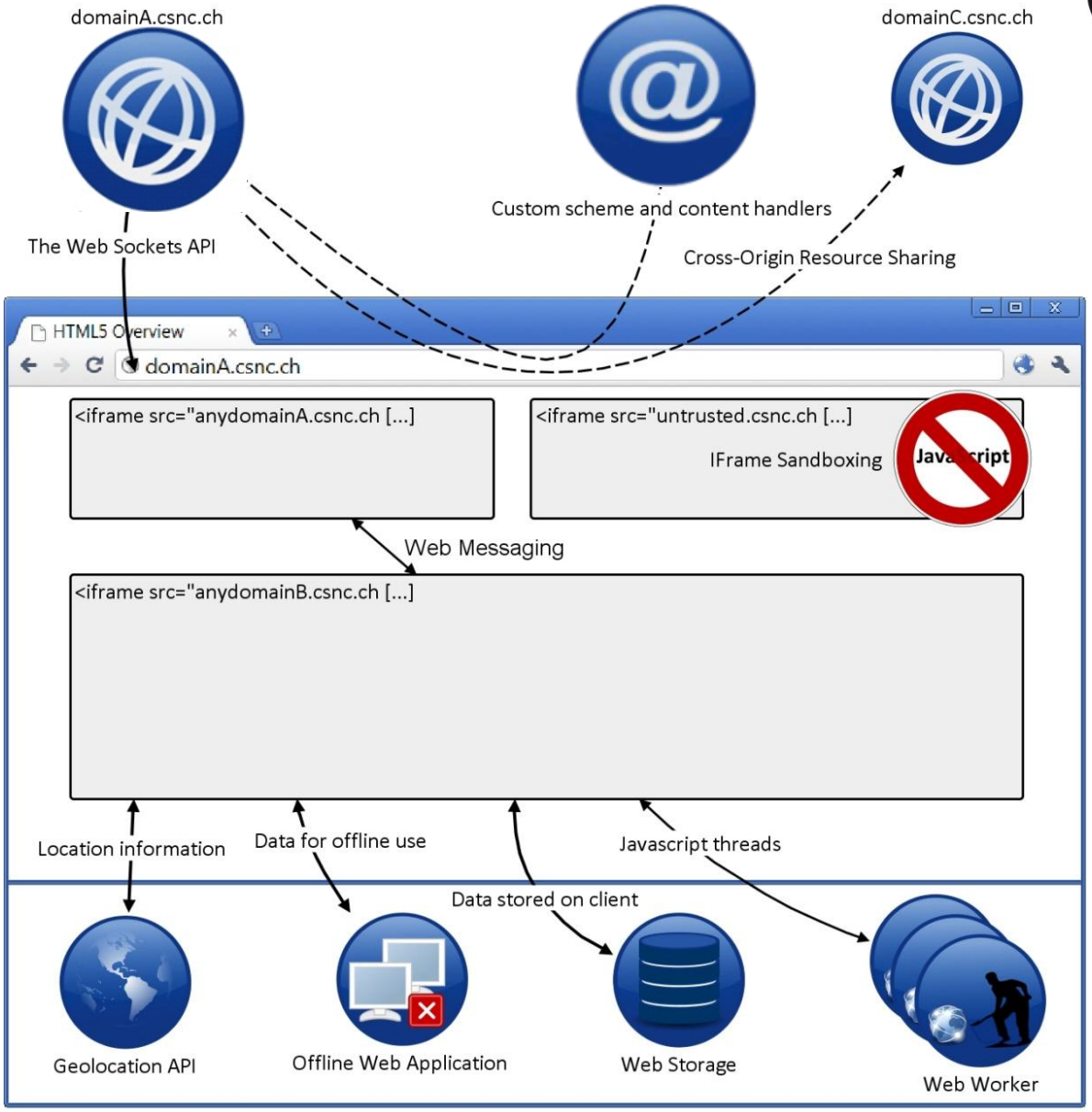
Countermeasures

The target in *postMessage()* should be defined explicitly and not set to *.

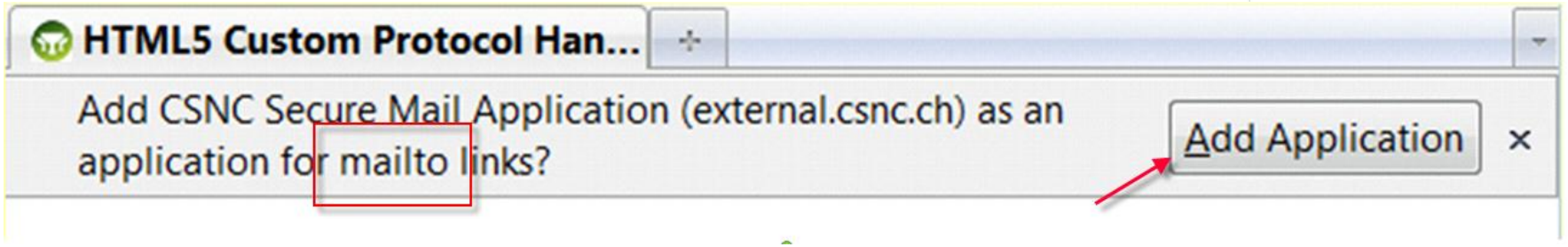
The receiving Iframe should not accept messages from any domain.
E.g. `e.origin == "http://internal.csnc.ch"`

The received message needs to be validated on the client to avoid malicious content being executed.

Custom scheme and content handlers



Custom scheme and content handlers



Stealing confidential data

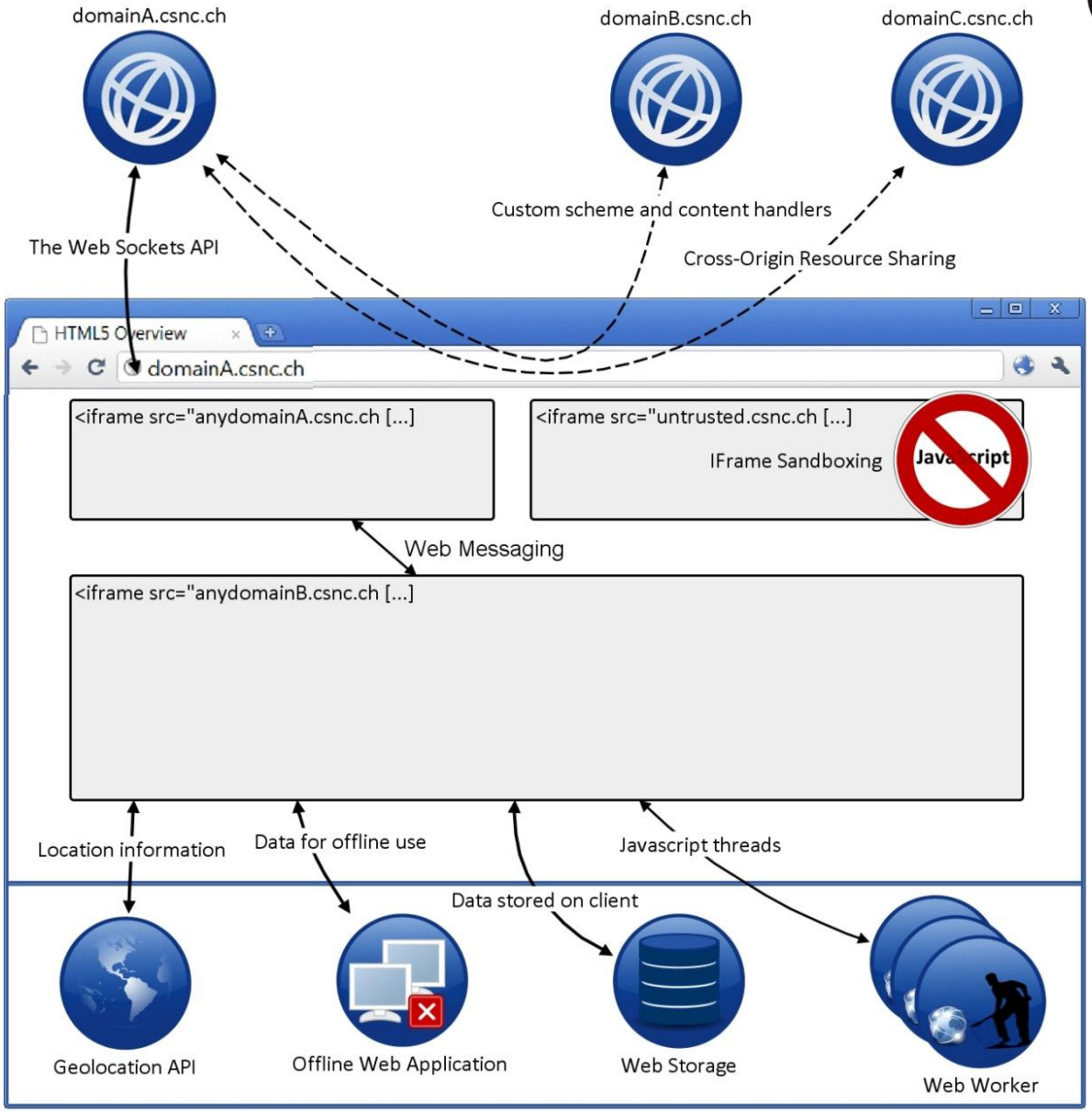
- An attacker tricks the user to register a malicious website as the e-mail protocol handler.
- Sending e-mails through this web application gives the attacker access to the content of the e-mail.

User Tracking

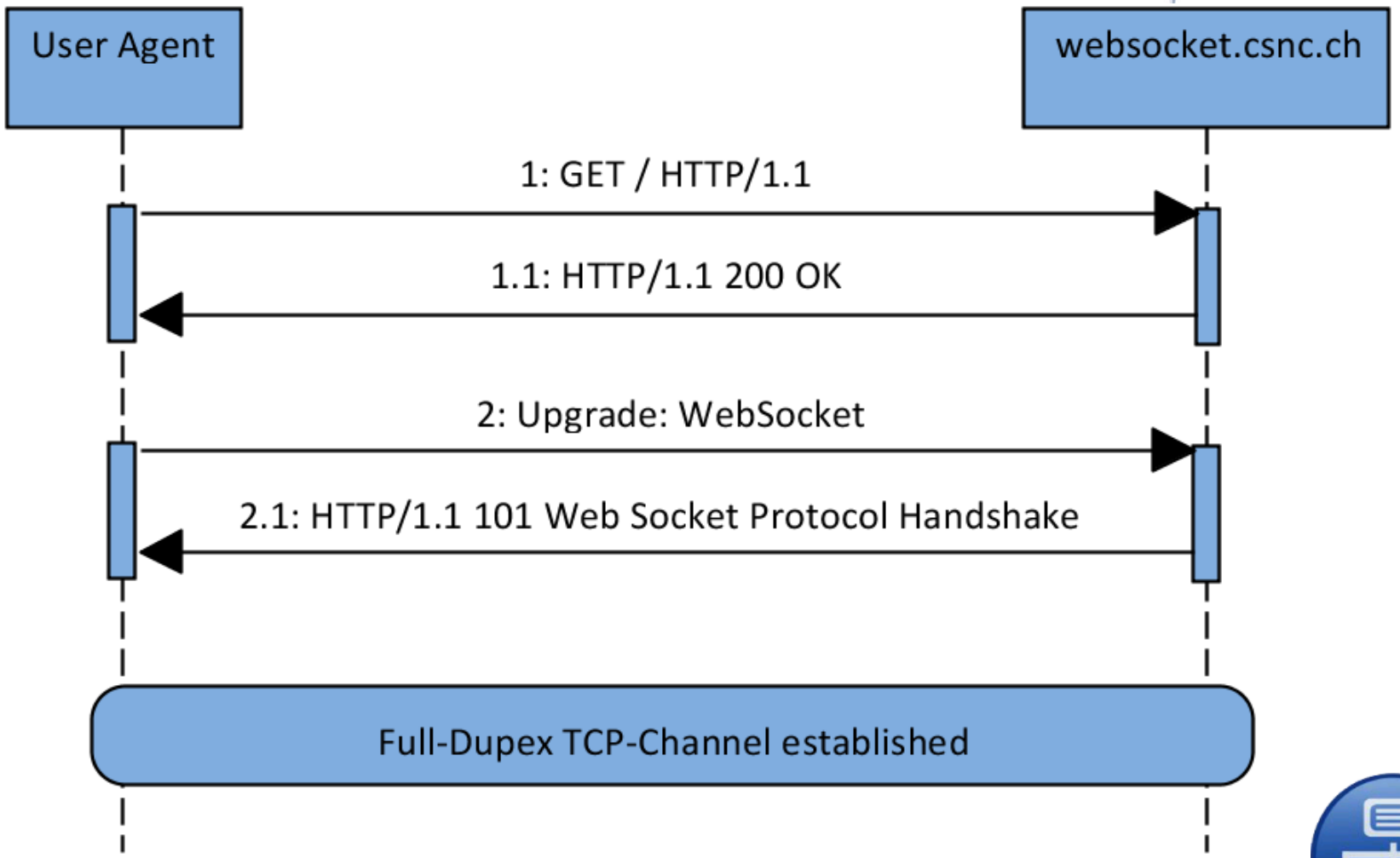
- Additional possibility to identify a user.
- Unique identifiers could be stored along with the protocol handler.

User-Training

Web Sockets API



Web Sockets API



Web Sockets API – Vuln. & Threats

Cache Poisoning

- A misunderstanding proxy could lead to a cache poisoning vulnerability.

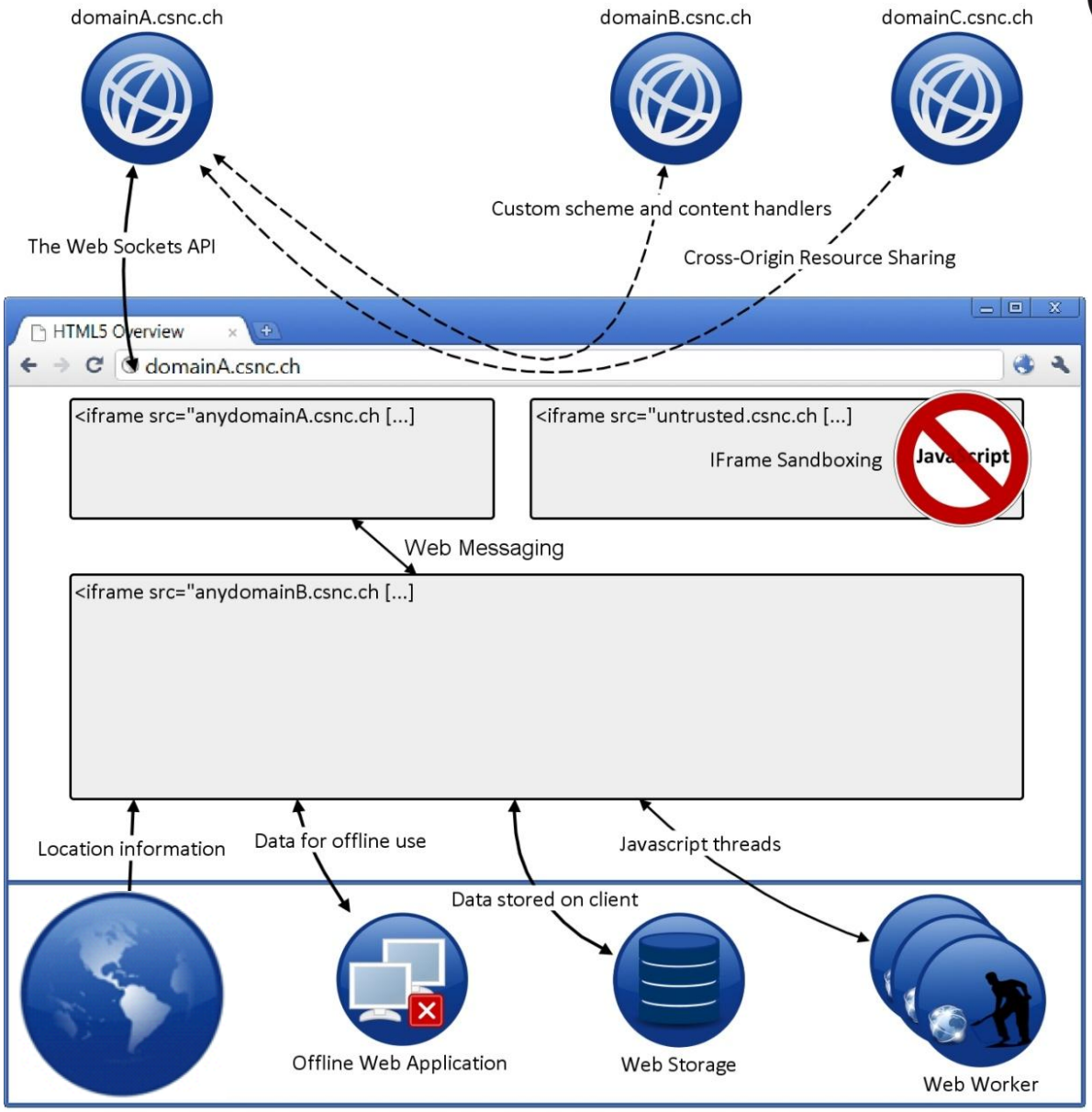
Scanning the internal network

- The browser of a victim can be used for port scanning of internal networks.

Establishing a remote shell

- Web Sockets can be used to establish a remote shell to a victim's browser.

Geolocation API



Geolocation API

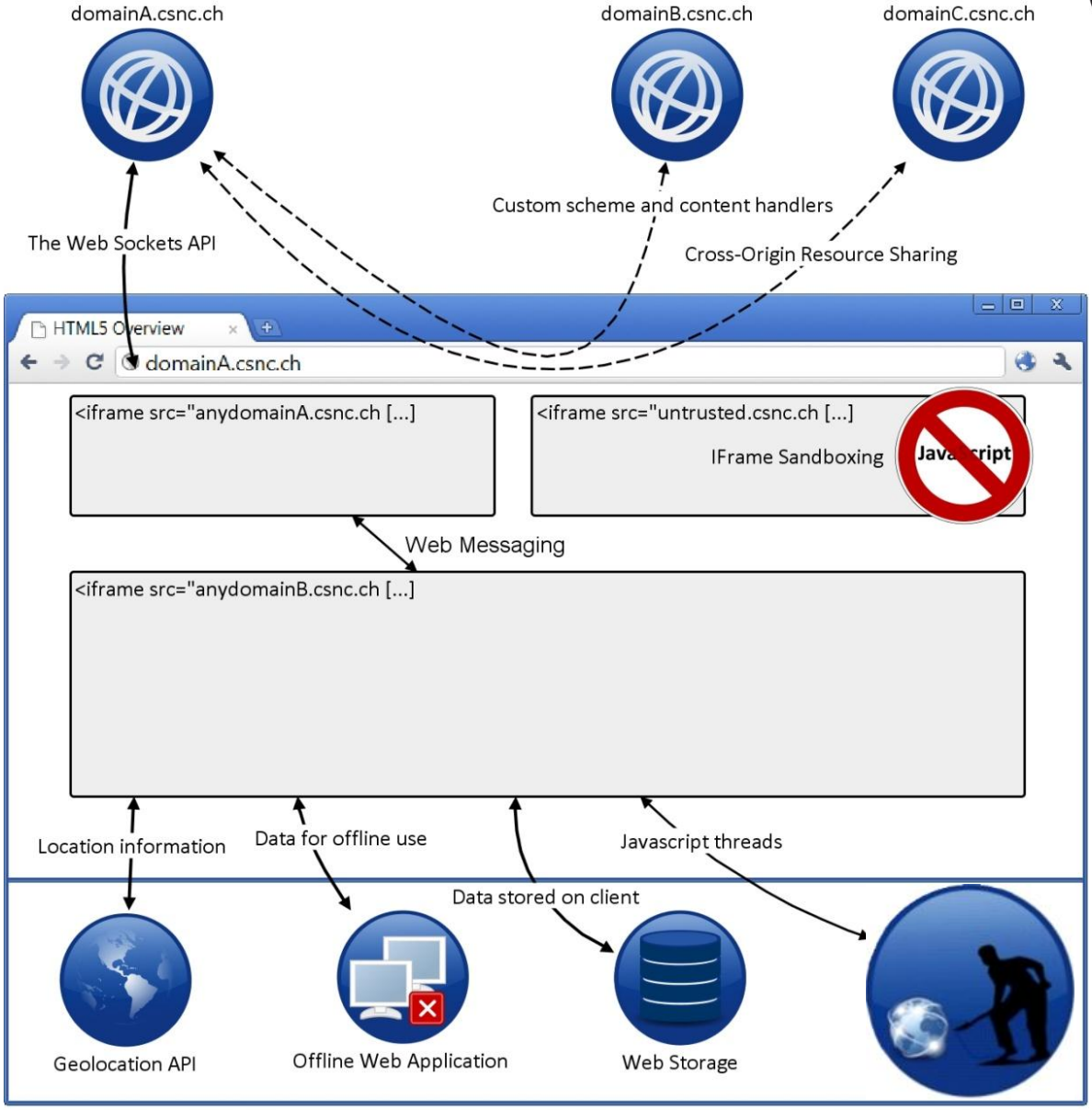
Finding your location: found you!

User Tracking

- User tracking based on the location of a user.
- If users are registered, their physical movement profile could be tracked.
- The anonymity of users could be broken.

User-Training

Web Workers


domainA.csnc.ch
domainB.csnc.ch
domainC.csnc.ch
The Web Sockets API
Custom scheme and content handlers
Cross-Origin Resource Sharing
HTML5 Overview
domainA.csnc.ch
<iframe src="anydomainA.csnc.ch [...]
<iframe src="untrusted.csnc.ch [...]
IFrame Sandboxing
Web Messaging
<iframe src="anydomainB.csnc.ch [...]
Location information
Data for offline use
Data stored on client
Javascript threads
Geolocation API
Offline Web Application
Web Storage

Web Workers

Web Workers provide the possibility for JavaScript to run in the background

Prior to Web Workers using JavaScript for long processing jobs was not feasible because

- it is slower than native code and
- the browsers freezes till the processing is completed

Web Workers alone are not a security issue.

But they can be used indirectly for launching work intensive attacks without the user noticing it.

Worst Case Scenarios

Web Workers = *Feature!*

Cracking Hashes in JS Cloud *(DEMO).*

Web Workers + Cross-Origin Resource Sharing =

Powerful DDoS attacks.

Web Workers + Cross-Origin Resource Sharing + Web Sockets =

Web-based Botnet.

… and much more …

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Some HTML5 features are the vulnerabilities themselves

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

XSS becomes even worse

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Use IE6

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

DEMO – Exploiting Cross-Origin Resource Sharing

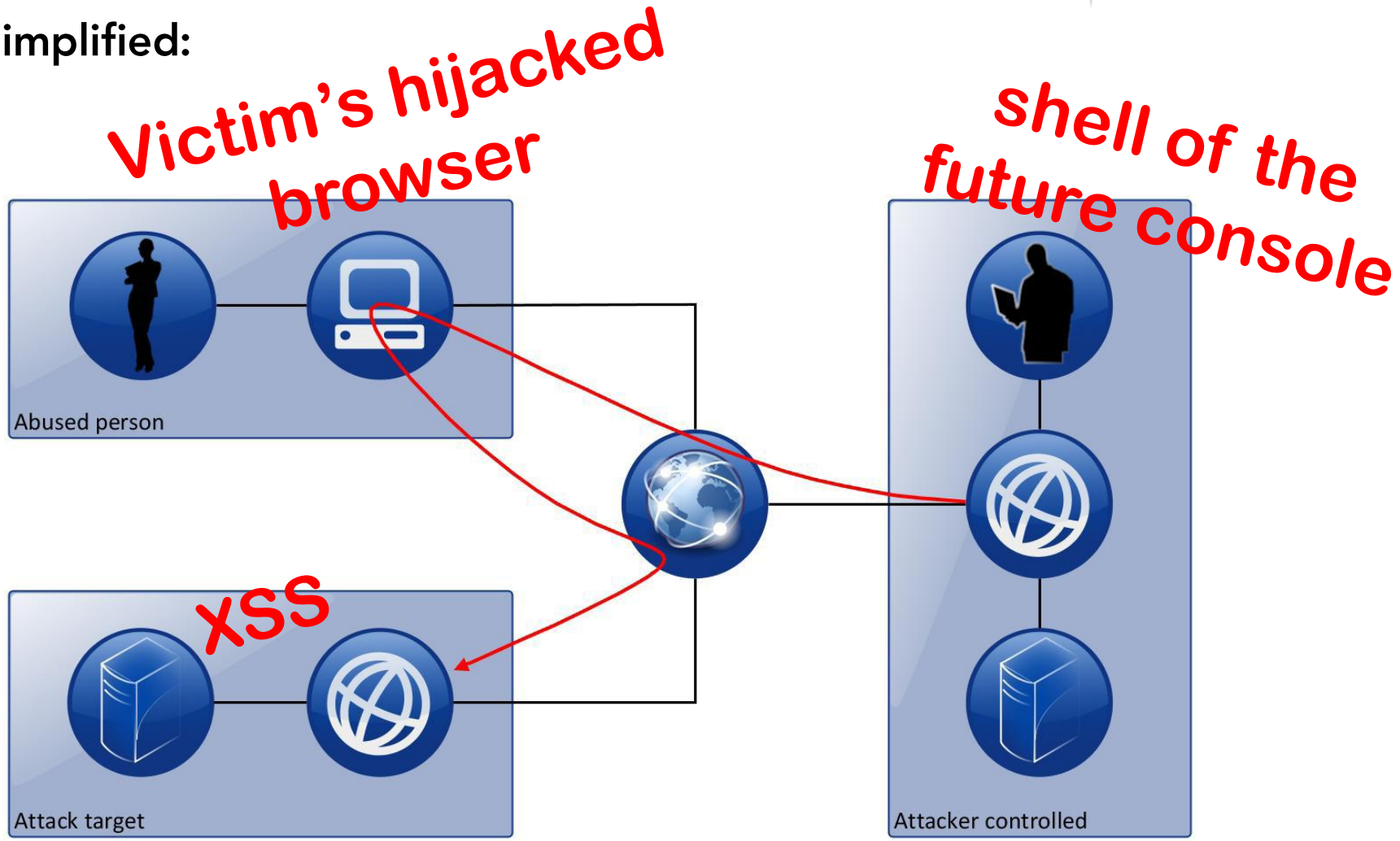
Shell of the Future

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

DEMO – CORS – Shell of the Future

Simplified:



DEMO – Exploiting Web Workers

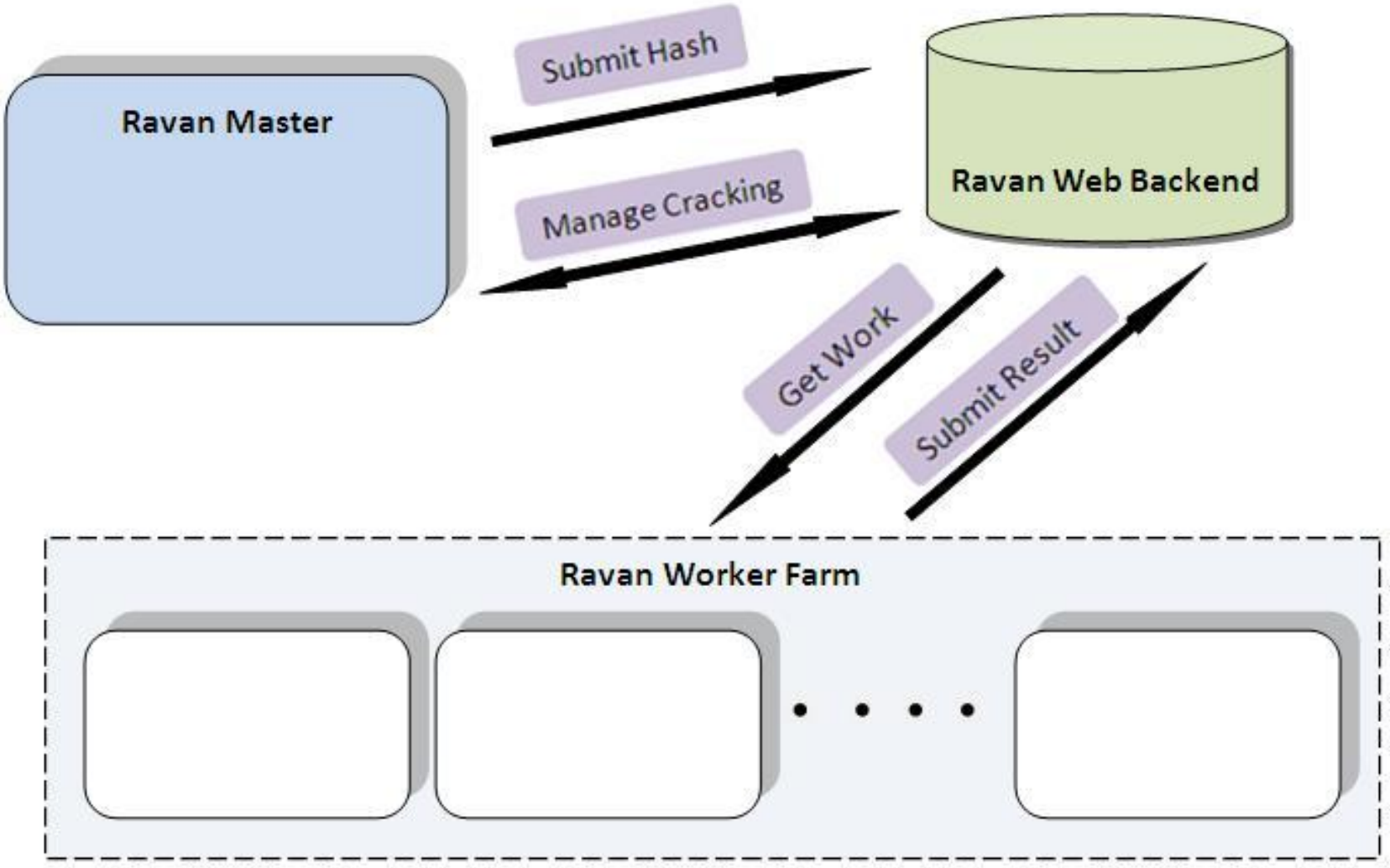
Ravan

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

DEMO – Web Workers – Ravan

http://www.andlabs.org/tools/ravan.html



DEMO – Web Workers – Ravan

96dd8092ed4f27024d44bb0ab5b08dd9

DEMO – Web Workers – Ravan

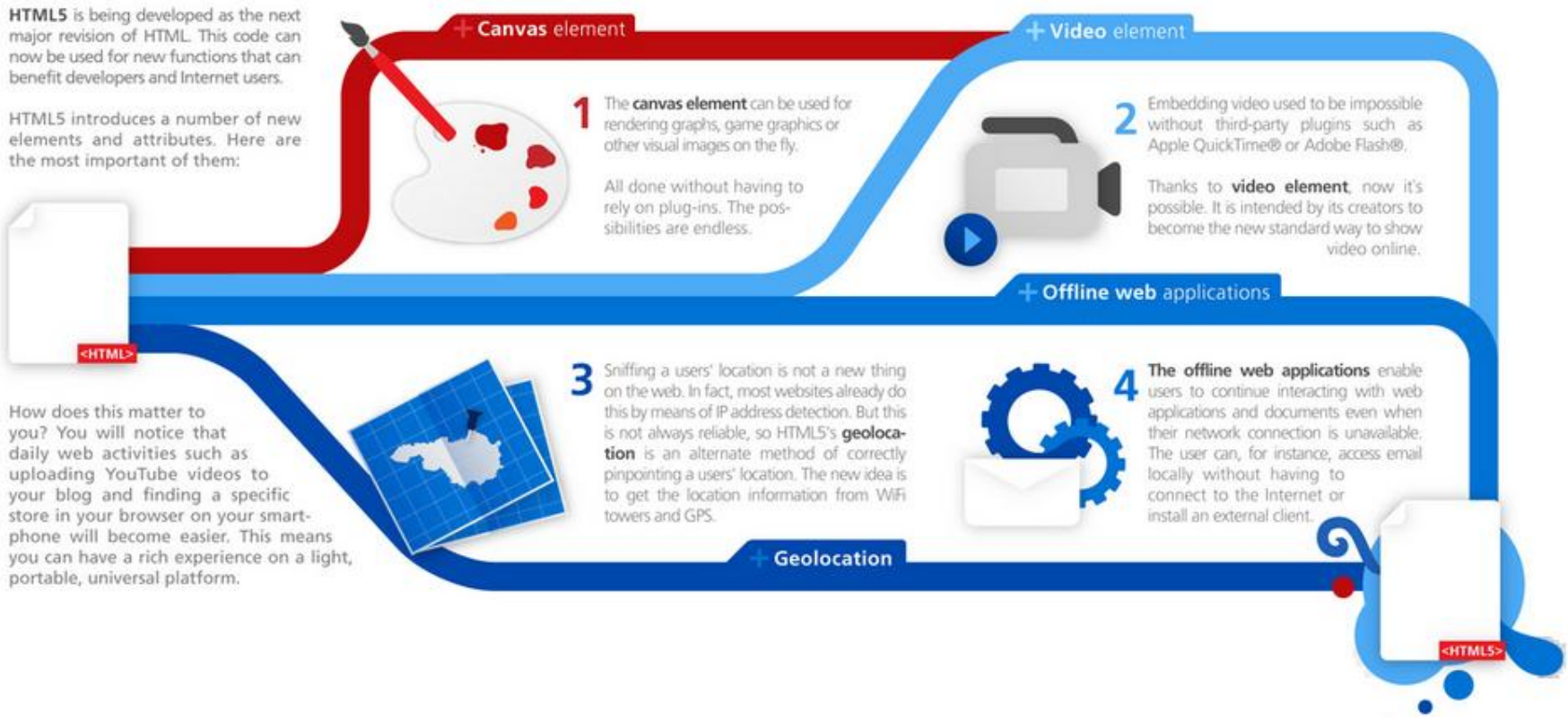
96dd8092ed4f27024d44bb0ab5b08dd9

DEMO – Web Workers – Ravan

ECBT

Erster Compass Beer Talk

Questions


HTML5 is being developed as the next major revision of HTML. This code can now be used for new functions that can benefit developers and Internet users.
HTML5 introduces a number of new elements and attributes. Here are the most important of them:
+ Canvas element
1 The canvas element can be used for rendering graphs, game graphics or other visual images on the fly.
All done without having to rely on plug-ins. The possibilities are endless.
+ Video element
2 Embedding video used to be impossible without third-party plugins such as Apple QuickTime® or Adobe Flash®.
Thanks to video element, now it's possible. It is intended by its creators to become the new standard way to show video online.
+ Offline web applications
<HTML>
How does this matter to you? You will notice that daily web activities such as uploading YouTube videos to your blog and finding a specific store in your browser on your smartphone will become easier. This means you can have a rich experience on a light, portable, universal platform.
3 Sniffing a users' location is not a new thing on the web. In fact, most websites already do this by means of IP address detection. But this is not always reliable, so HTML5's geolocation is an alternate method of correctly pinpointing a users' location. The new idea is to get the location information from WiFi towers and GPS.
4 The offline web applications enable users to continue interacting with web applications and documents even when their network connection is unavailable. The user can, for instance, access email locally without having to connect to the Internet or install an external client.
+ Geolocation
<HTML5>

References

- Michael Schmidt, master thesis „HTML 5 Web Security“, 31st March 2011
- Lavakumar Kuppan, Attack and Defense Labs, http://www.andlabs.org
- W3C, HTML5, A vocabulary and associated APIs for HTML and XHTML, http://dev.w3.org/html5/spec/Overview.html