HTML5 Web Security

Thomas Röthlisberger – IT Security Analyst

thomas.roethlisberger@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 is 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

Agenda

What is HTML5?

Vulnerabilities, Threats & Countermeasures

Conclusion

Demo CORS

Demo Web Workers

Quiz and Q&A

The Voting Device

Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

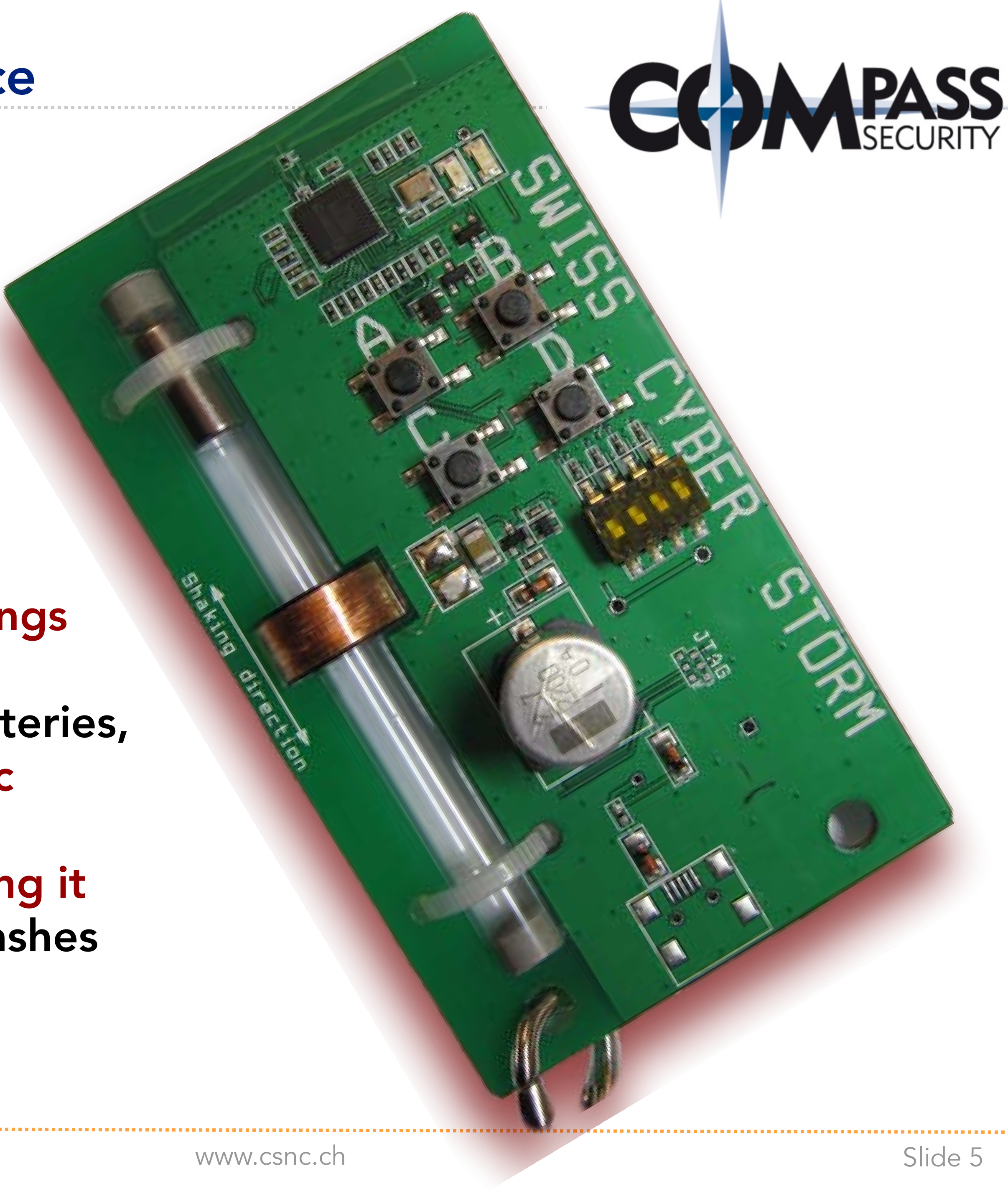
Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

The Voting Device

It enables you to participate on votings

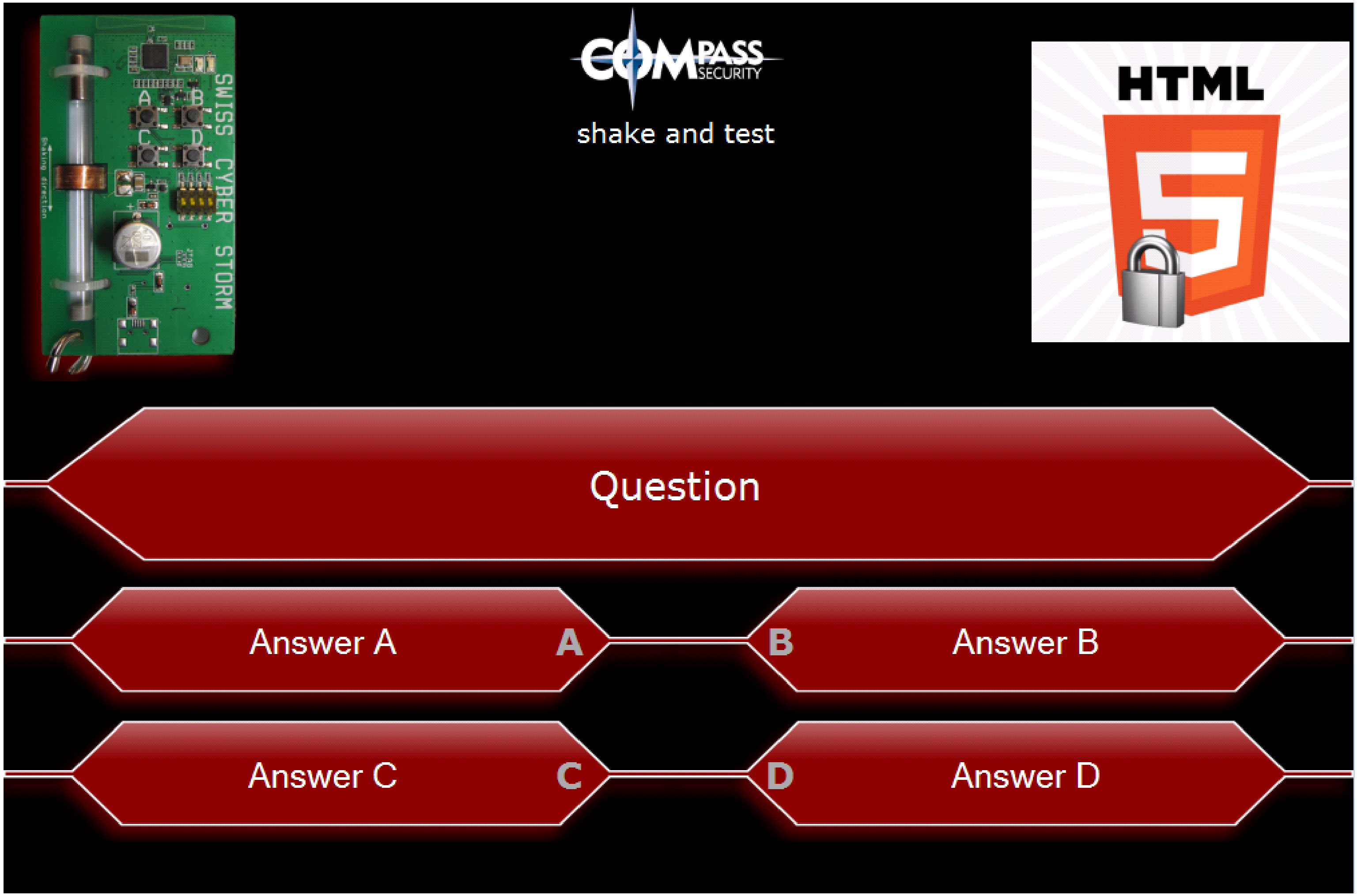
The device has no batteries, so it works autarkic

You power it by shaking it until green light flashes



The Voting

Let's give it a try…



shake and test

Question

Answer A A

B Answer B

Answer C C

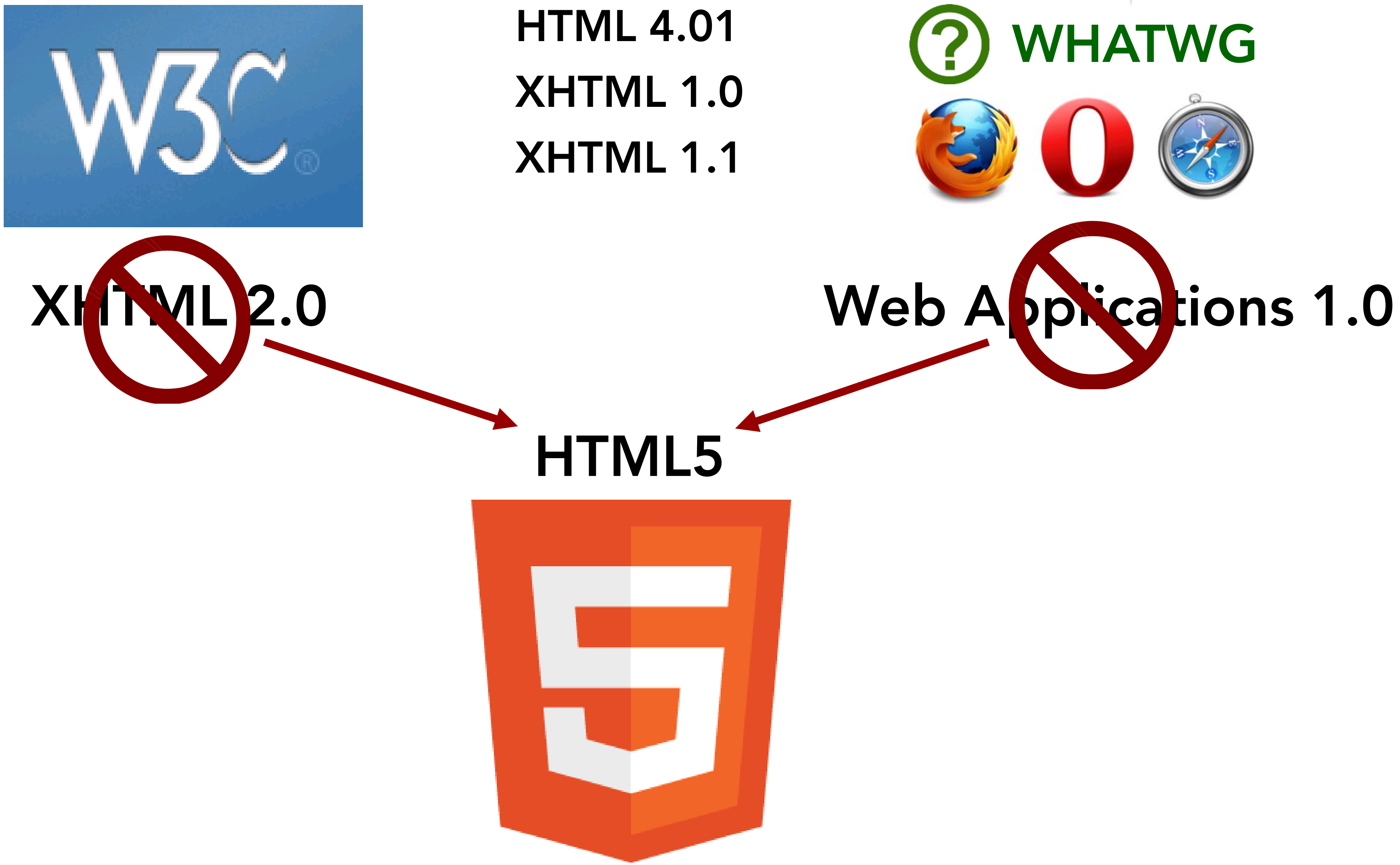
D Answer D

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

History



HTML 4.01

XHTML 1.0

XHTML 1.1

WHATWG

XHTML 2.0

Web Applications 1.0

HTML5

History

HTML5 is not finished!

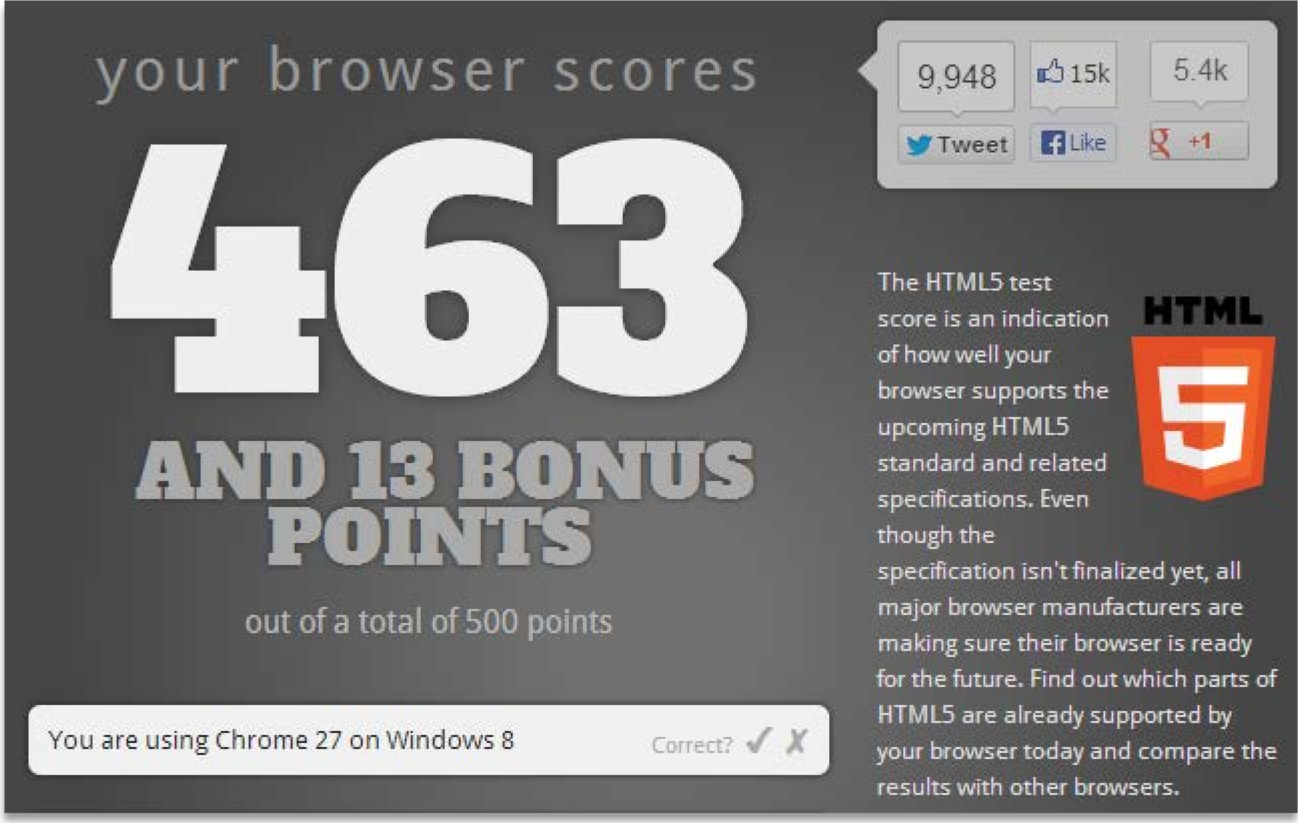
The specification achieved CANDIDATE RECOMMENDATION status on 17 December 2012.

However, it is still a draft version and may be updated.

THE FUTURE
ACCORDING TO GOOGLE SEARCH RESULTS
2021
US DEBT REACHES 97% OF GDP
US UNEMPLOYMENT FALLS TO 2.8%
RESTORED CALIPHATE UNIFIES MIDDLE EAST
LAKE MEAD EVAPORATES
KILIMANJARO SNOW-FREE
2022
HTML 5 FINISHED
NEWSPAPERS BECOME OBSOLETE AND DIE OUT
JESUS RETURNS TO EARTH (AGAIN)
2023
US DEBT PASSES 100% OF GDP
ALL UNPROTECTED ANCIENT FORESTS GONE FROM PACIFIC NORTHWEST

http://xkcd.com/887/

HTML5 TEST - http://html5test.com/



your browser scores

463

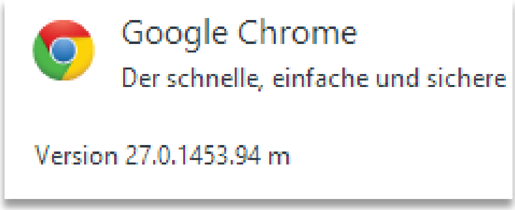
AND 13 BONUS POINTS

out of a total of 500 points

You are using Chrome 27 on Windows 8

The HTML5 test score is an indication of how well your browser supports the upcoming HTML5 standard and related specifications. Even though the specification isn't finalized yet, all major browser manufacturers are making sure their browser is ready for the future. Find out which parts of HTML5 are already supported by your browser today and compare the results with other browsers.

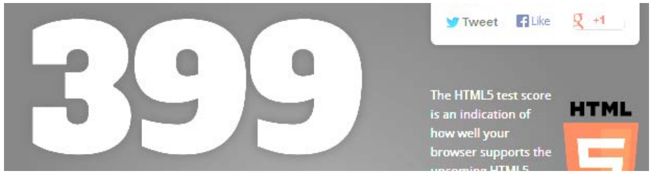
out of a total of 500 points



Google Chrome

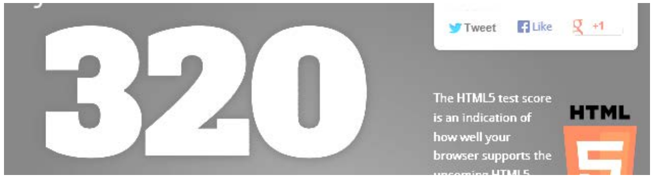
Der schnelle, einfache und sichere

Version 27.0.1453.94 m



399

The HTML5 test score is an indication of how well your browser supports the

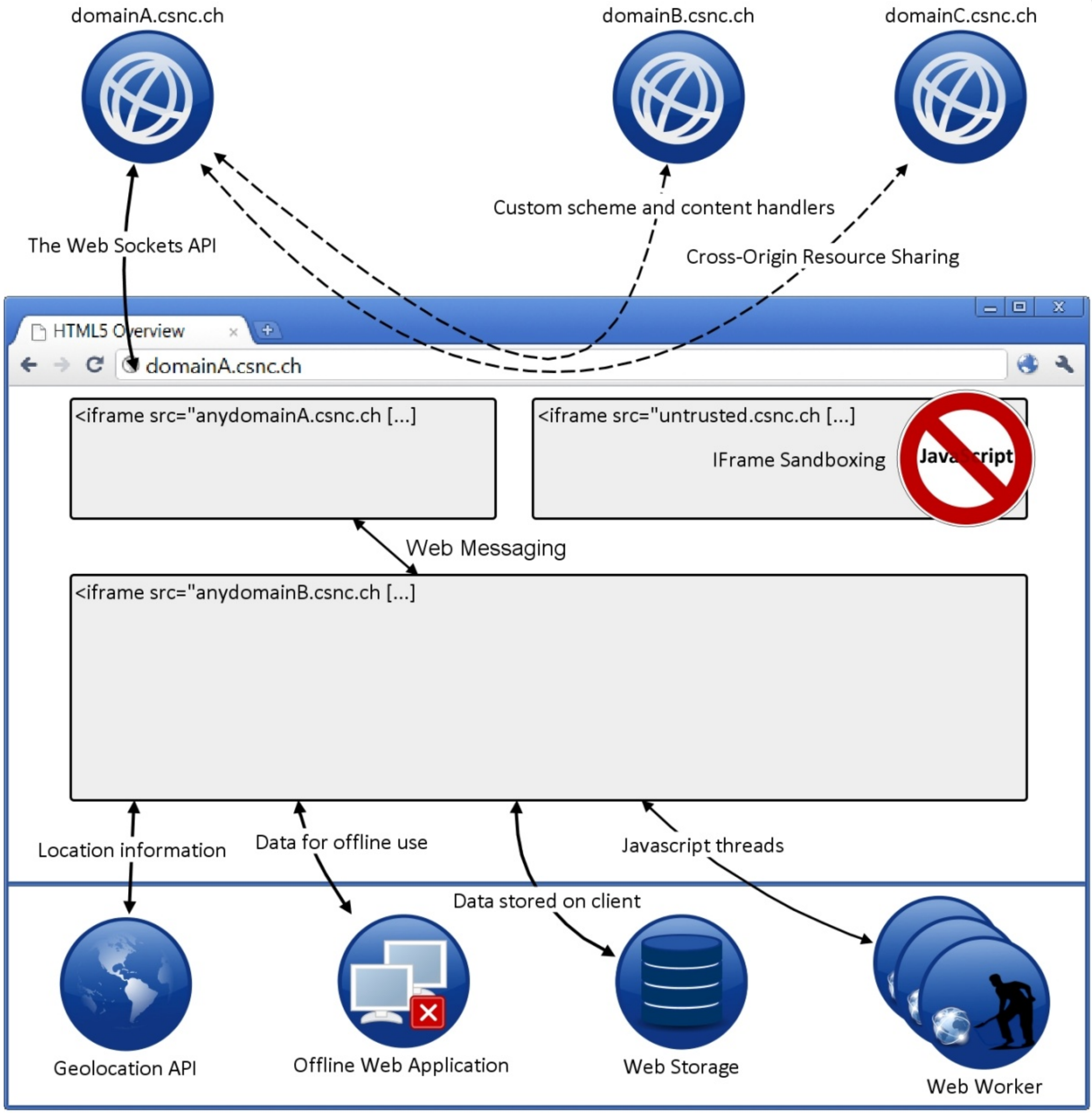


320

The HTML5 test score is an indication of how well your browser supports the

Version: 10.0.9200.16580

Overview

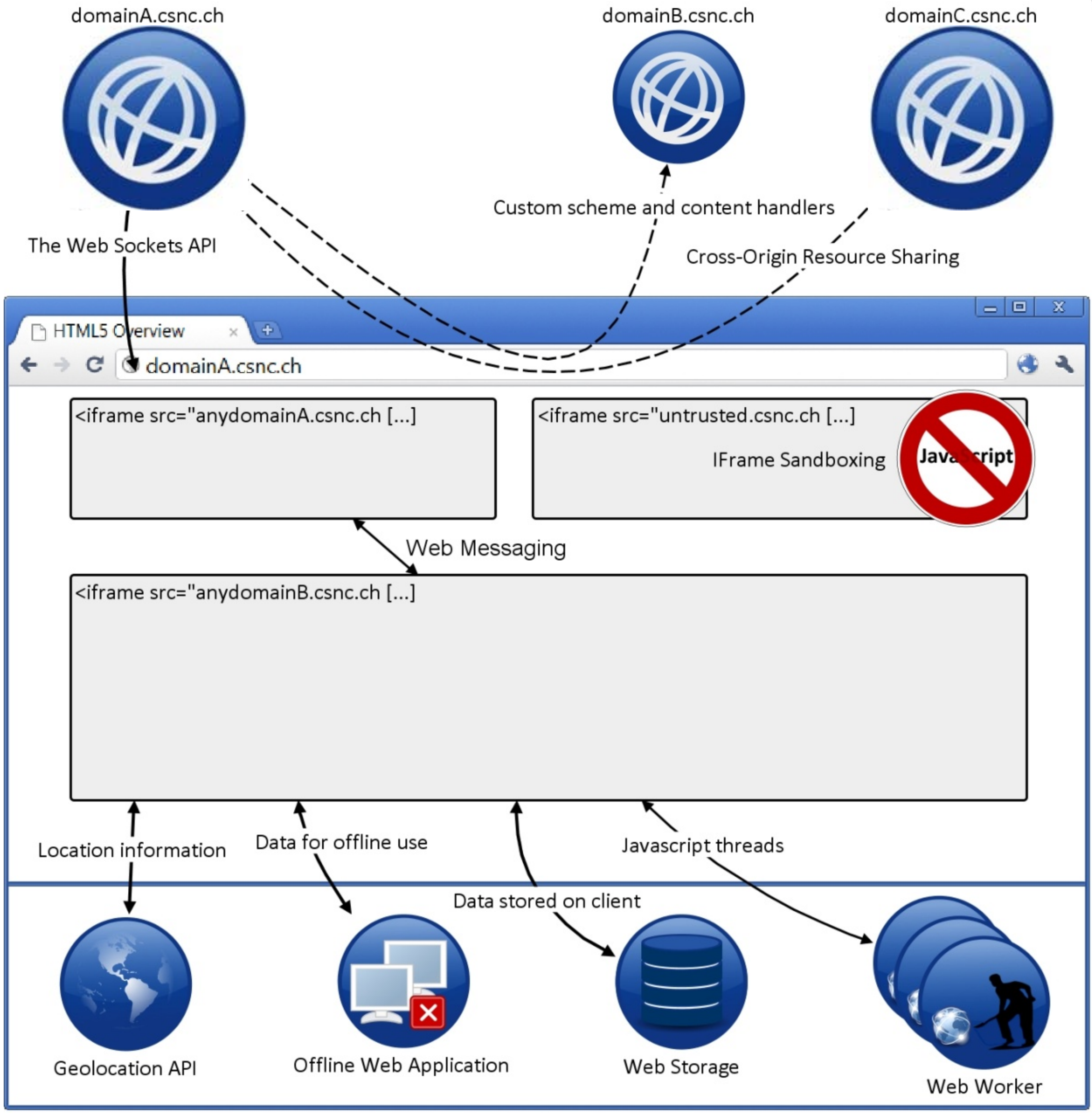

domainA.csnc.ch
domainB.csnc.ch
domainC.csnc.ch
The Web Sockets API
Custom scheme and content handlers
Cross-Origin Resource Sharing
HTML5 Overview
domainA.csnc.ch
<iframe src="anydomainA.csnc.ch [...]
<iframe src="untrusted.csnc.ch [...]
IFrame Sandboxing
JavaScript
Web Messaging
<iframe src="anydomainB.csnc.ch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

Vulnerabilities, Threats and Countermeasures *(if any)*

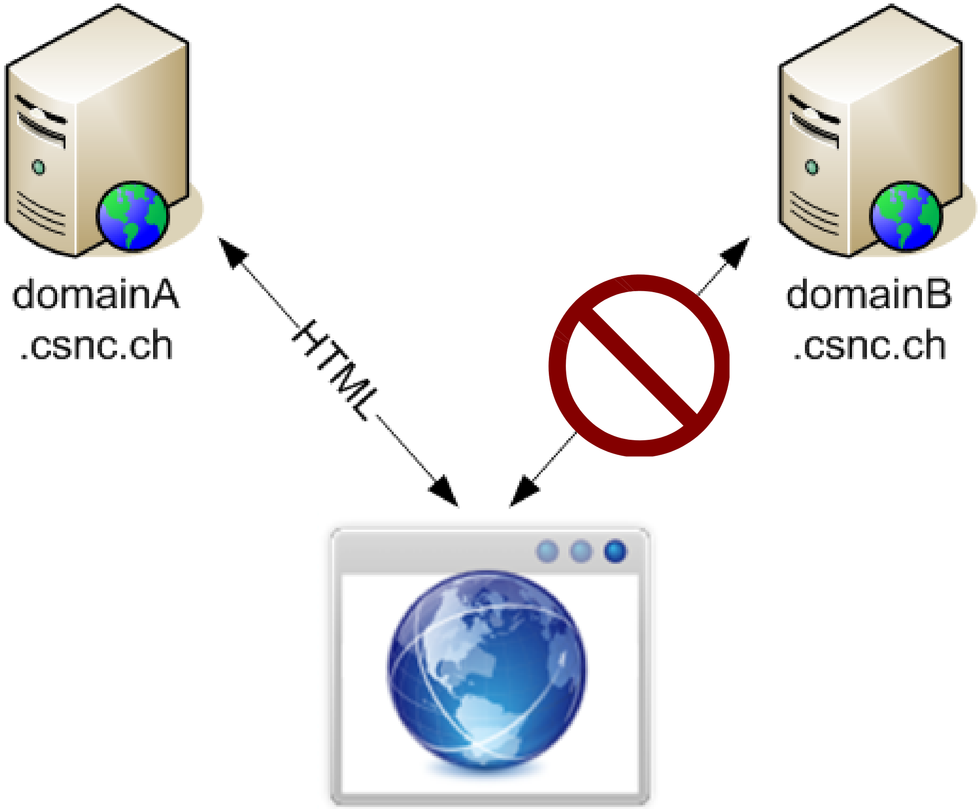
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

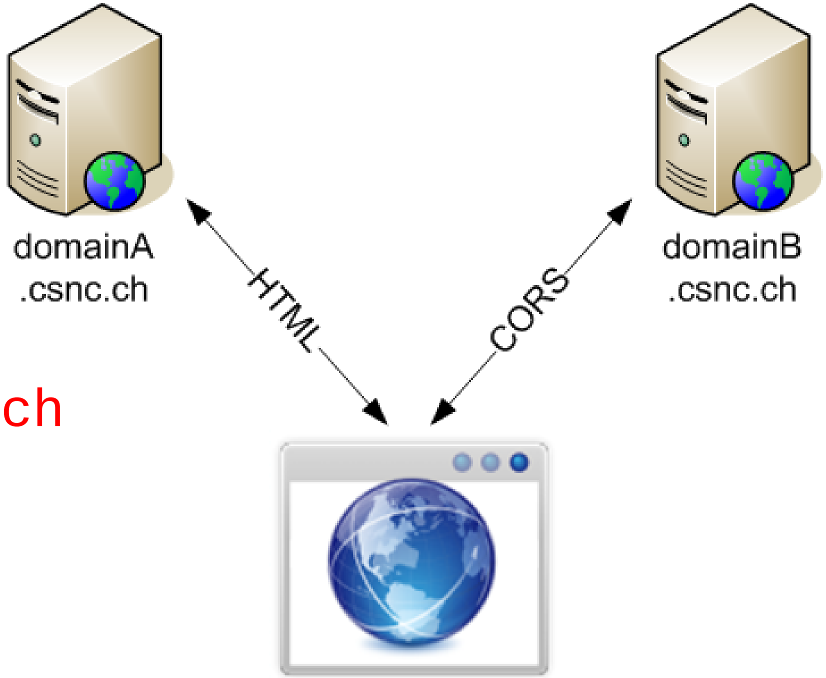
Cross-Origin Resource Sharing



Cross-Origin Resource Sharing I



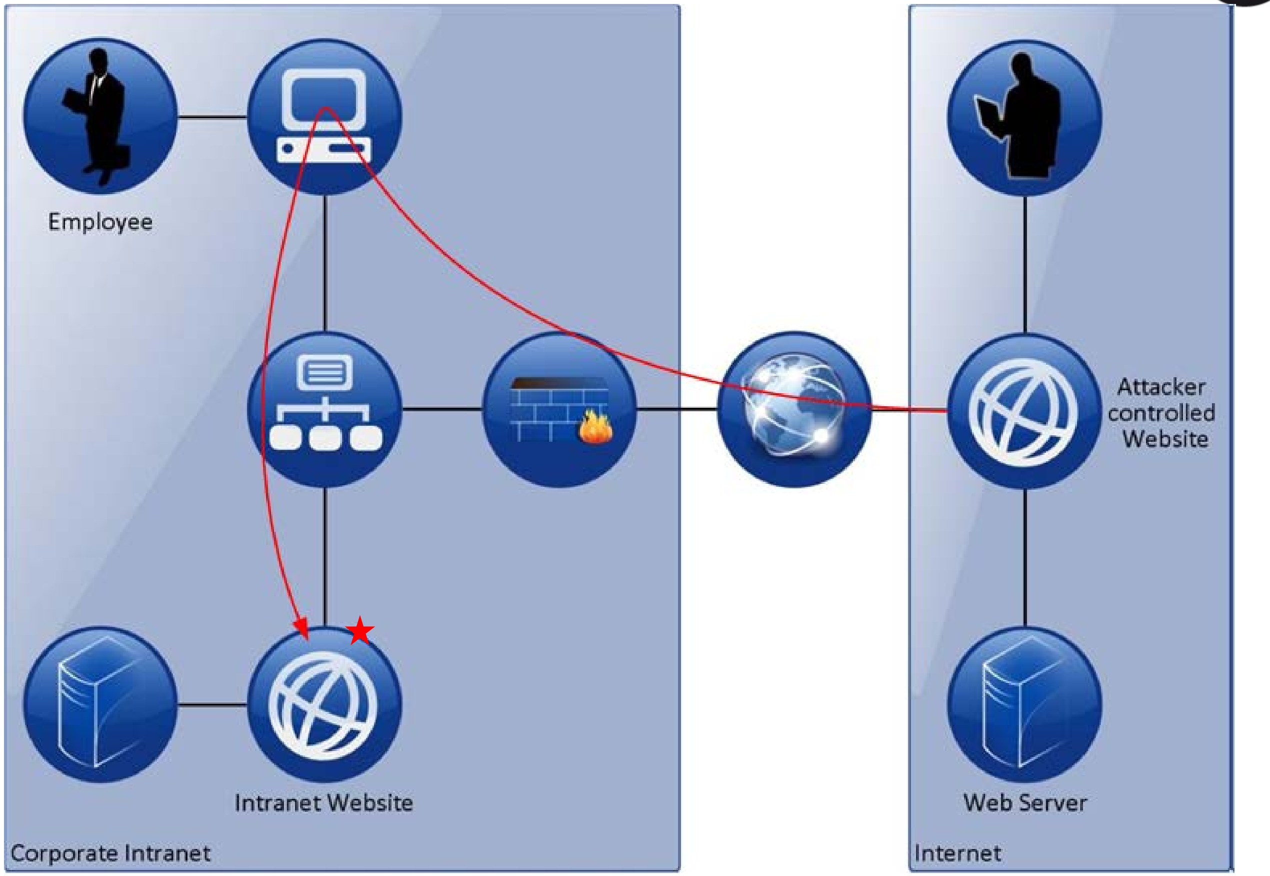
Cross-Origin Resource Sharing II



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

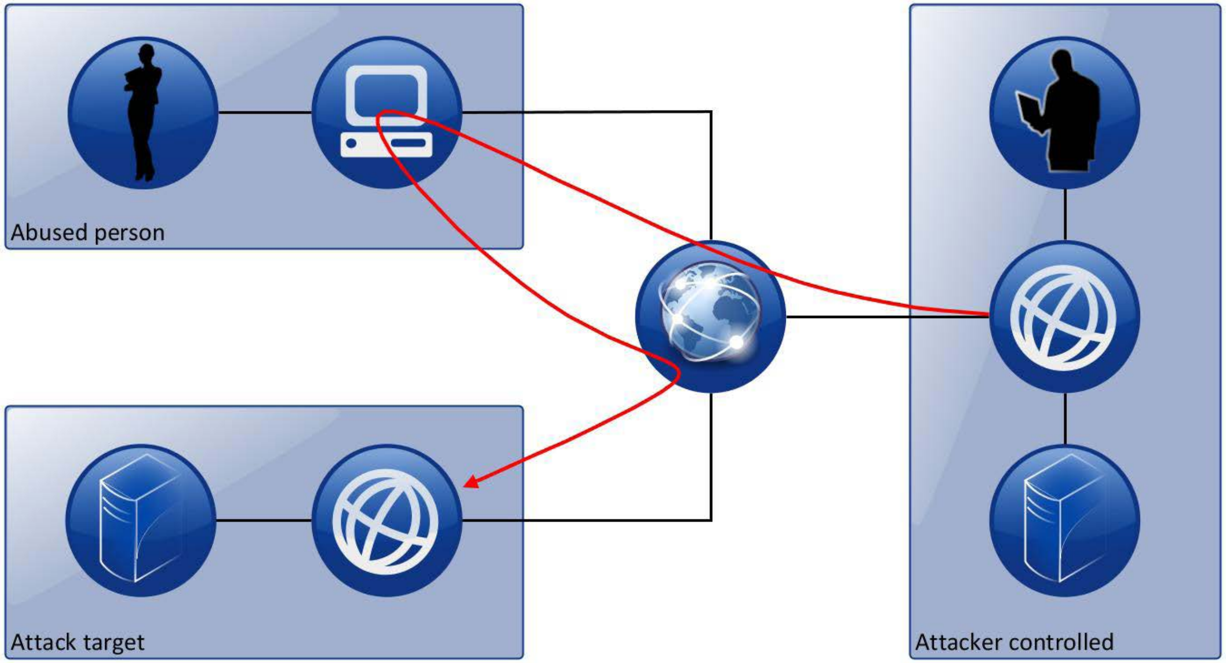
```
HTTP/1.1 200 OK
Content-Type: text/html
Access-Control-Allow-Origin: http://domainA.csnc.ch
```

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

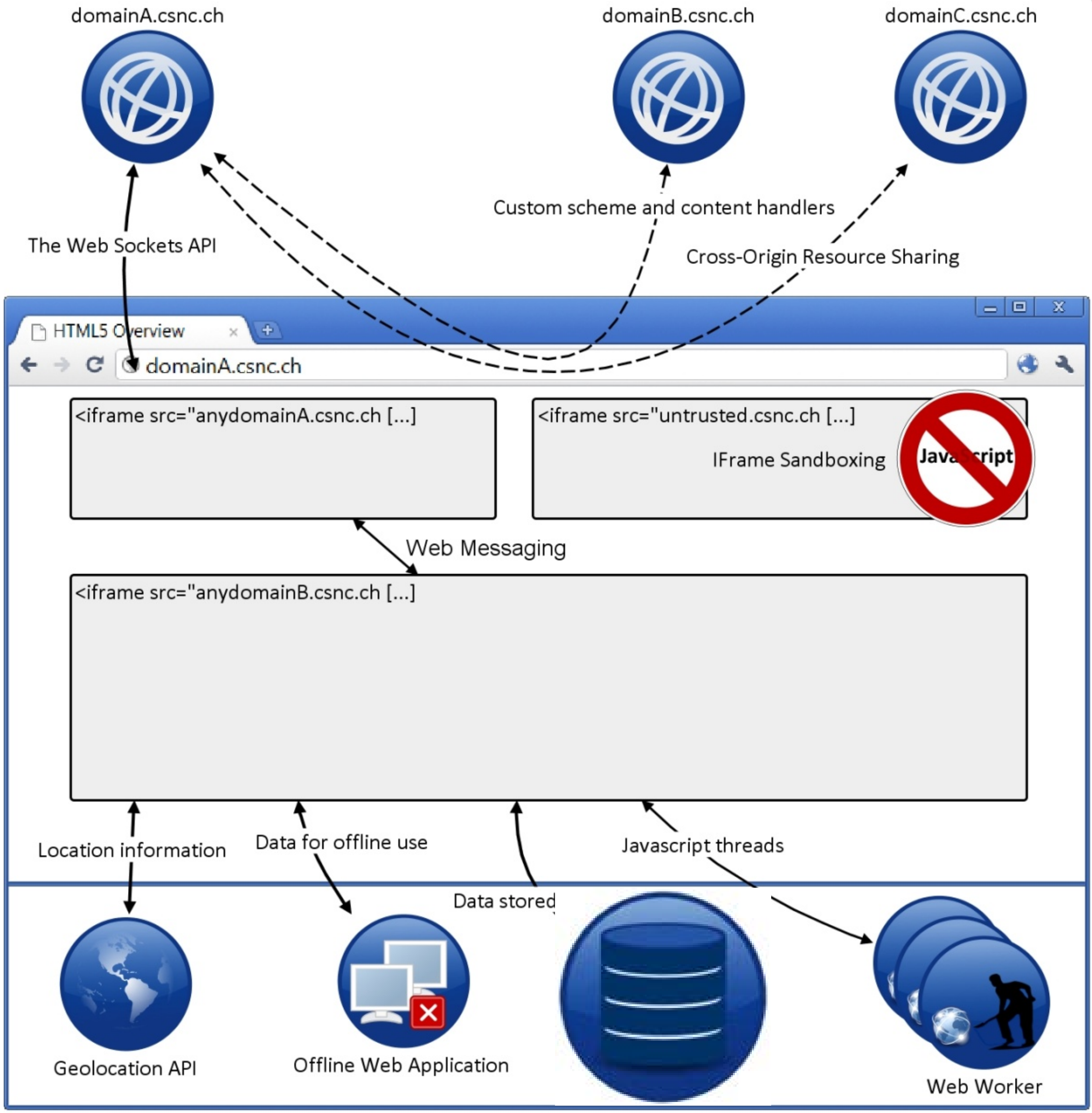
Use the `Access-Control-Allow-Origin` header to restrict the allowed domains.

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

JavaScript

Web Messaging

<iframe src="anydomainB.csnc.ch [...]

Location information

Data for offline use

Data stored

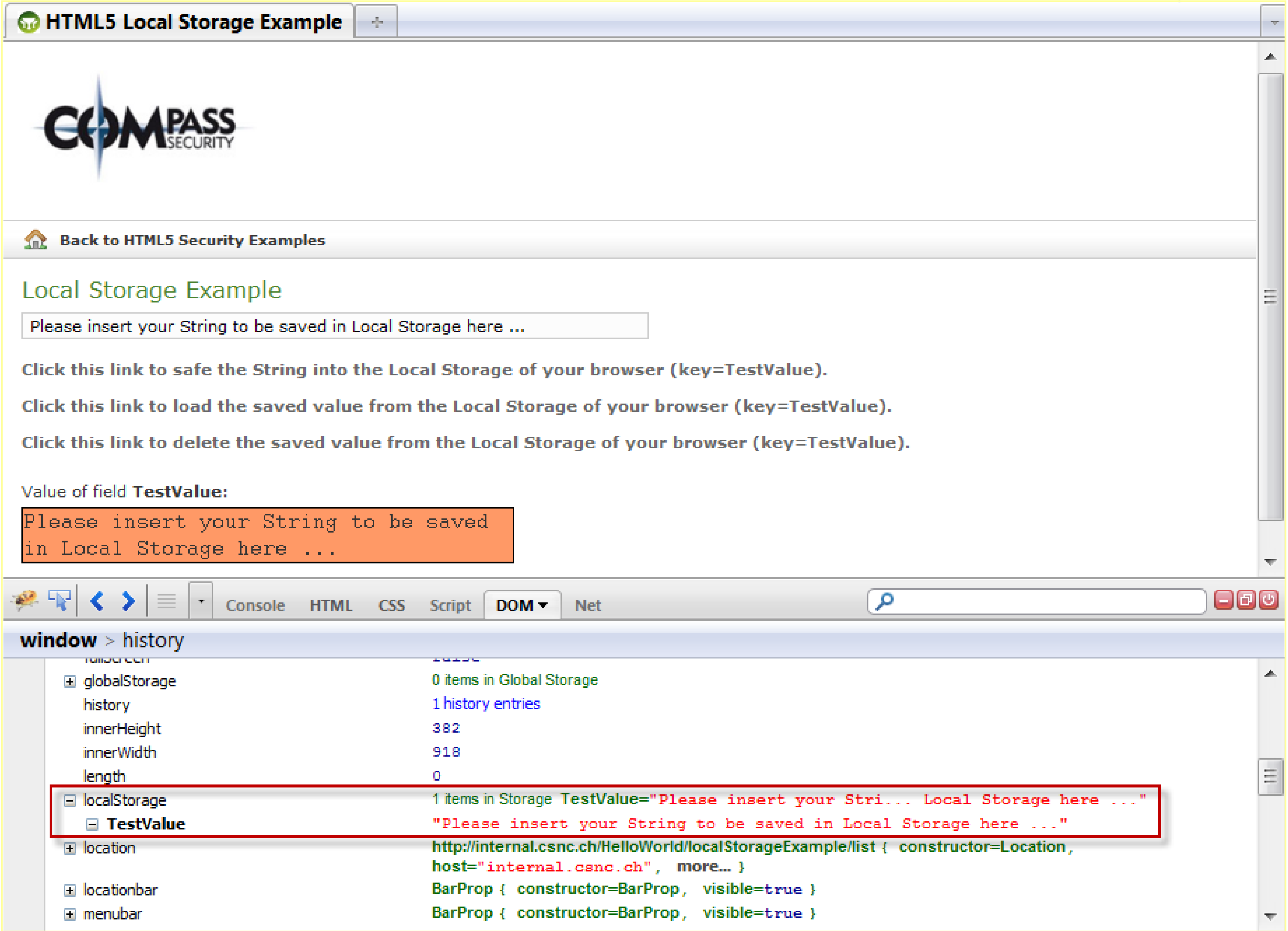
Javascript threads

Geolocation API

Offline Web Application

Web Worker

Web Storage



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 ...
```

```
⊞ 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

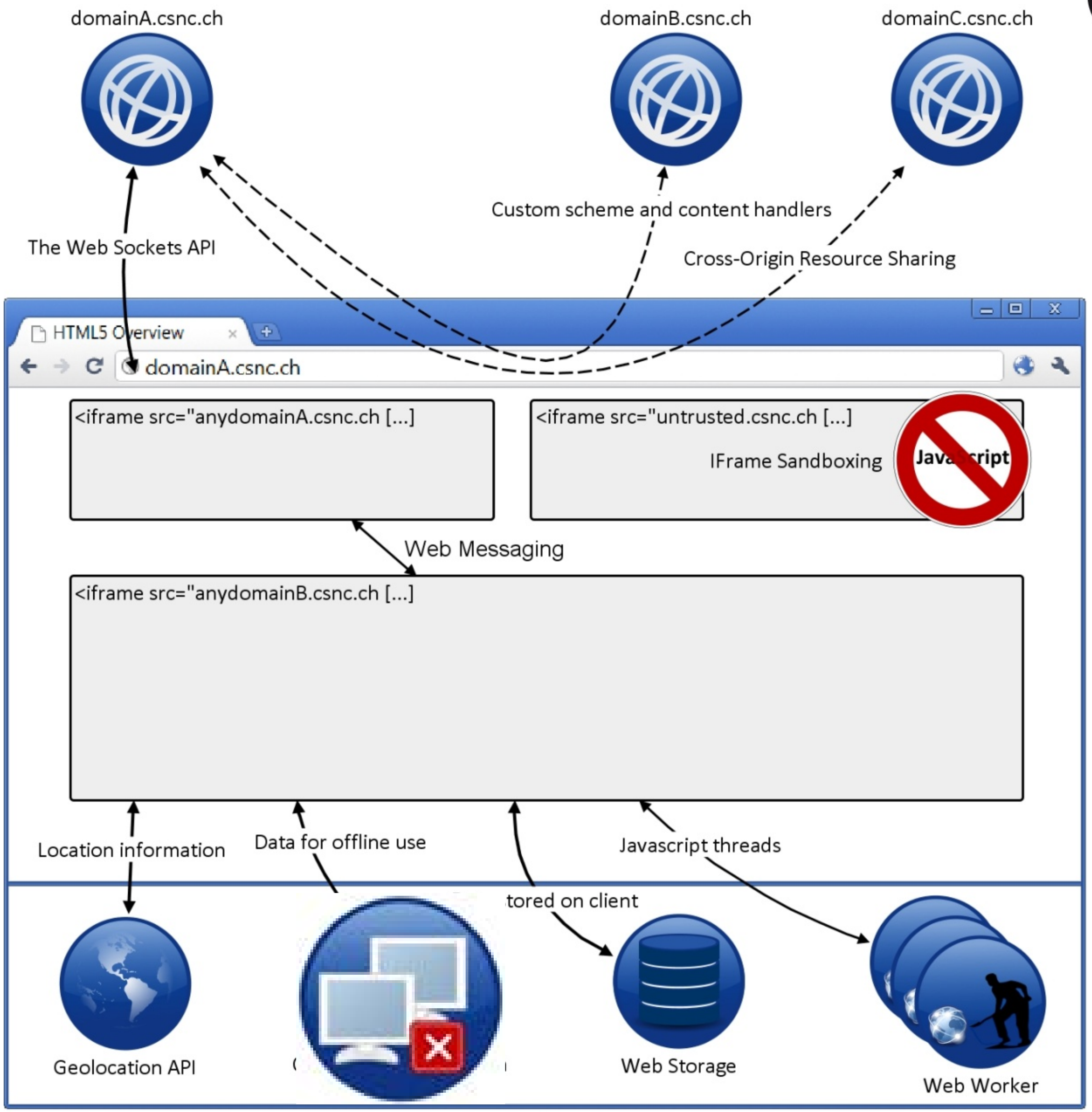
- Attack vectors can be stored persistently in the victim’s browser.

Countermeasures

Use cookies instead of Local Storage for session handling.

Do not store sensitive data in Local Storage.

Offline Web Application



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

Javascript threads

tored on client

Geolocation API

Web Storage

Web Worker

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.

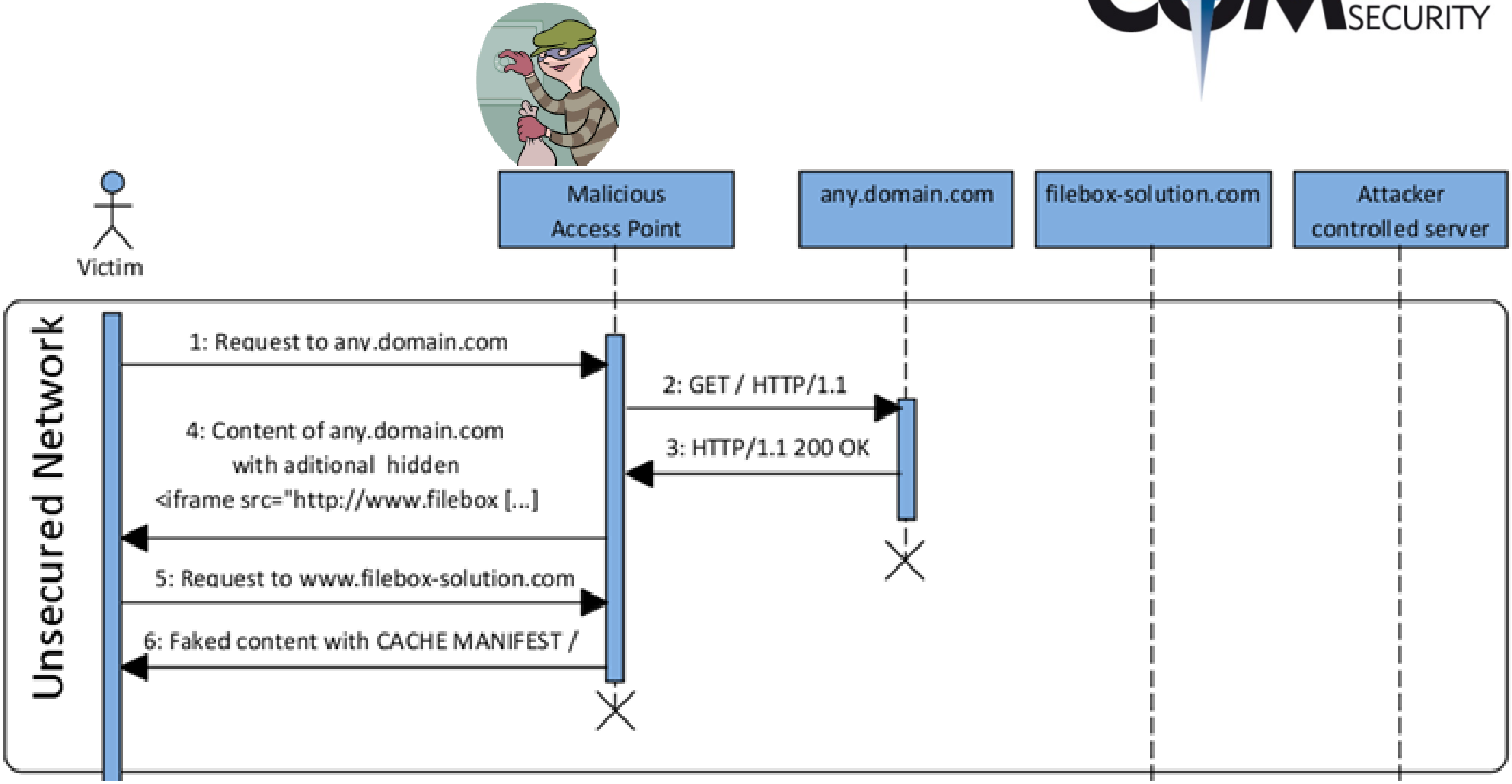
Persistent attack vectors

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

User Tracking

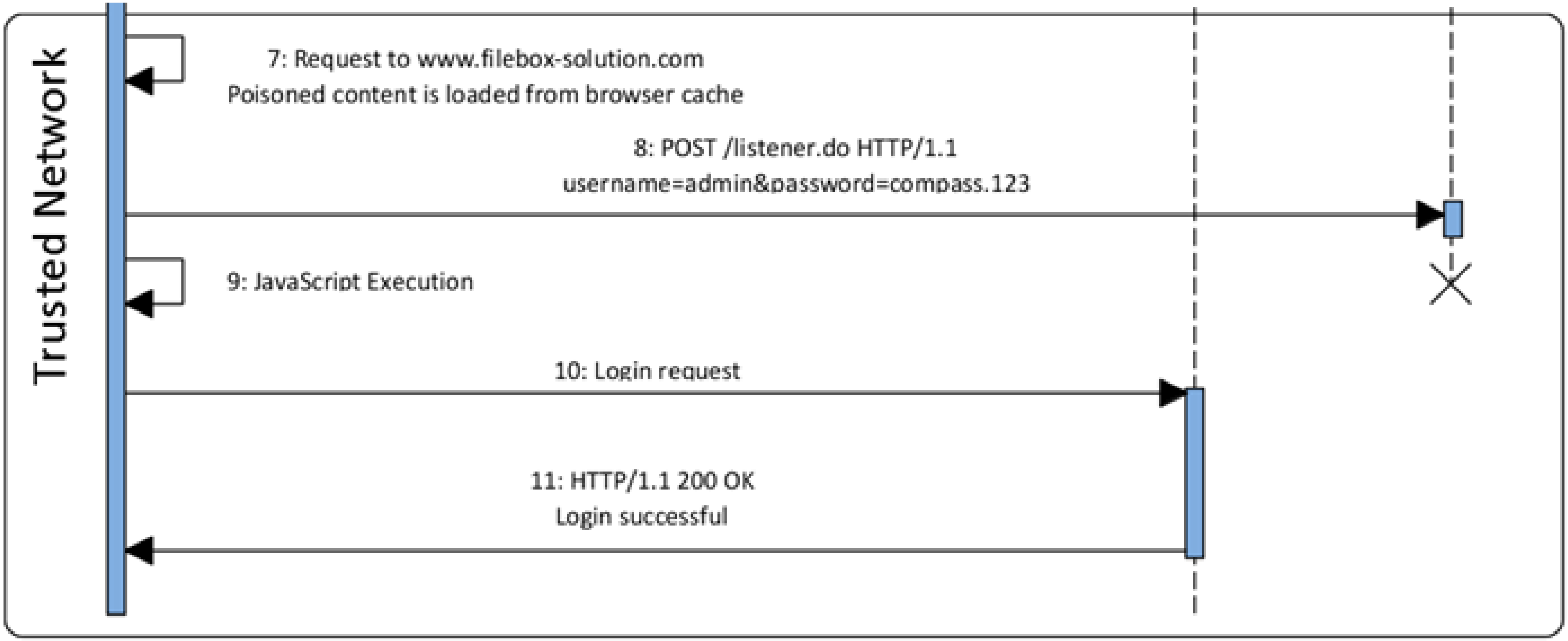
- Additional possibility to identify a user.
- Unique identifiers could be stored along with the cached files.

Offline Web Application – Attack 1/2



Victim
Malicious Access Point
any.domain.com
filebox-solution.com
Attacker controlled server
Unsecured Network
1: Request to any.domain.com
2: GET / HTTP/1.1
3: HTTP/1.1 200 OK
4: Content of any.domain.com with aditional hidden <iframe src="http://www.filebox [...]
5: Request to www.filebox-solution.com
6: Faked content with CACHE MANIFEST /

Offline Web Application – Attack 2/2



7: Request to www.filebox-solution.com
Poisoned content is loaded from browser cache

8: POST /listener.do HTTP/1.1
username=admin&password=compass.123

9: JavaScript Execution

10: Login request

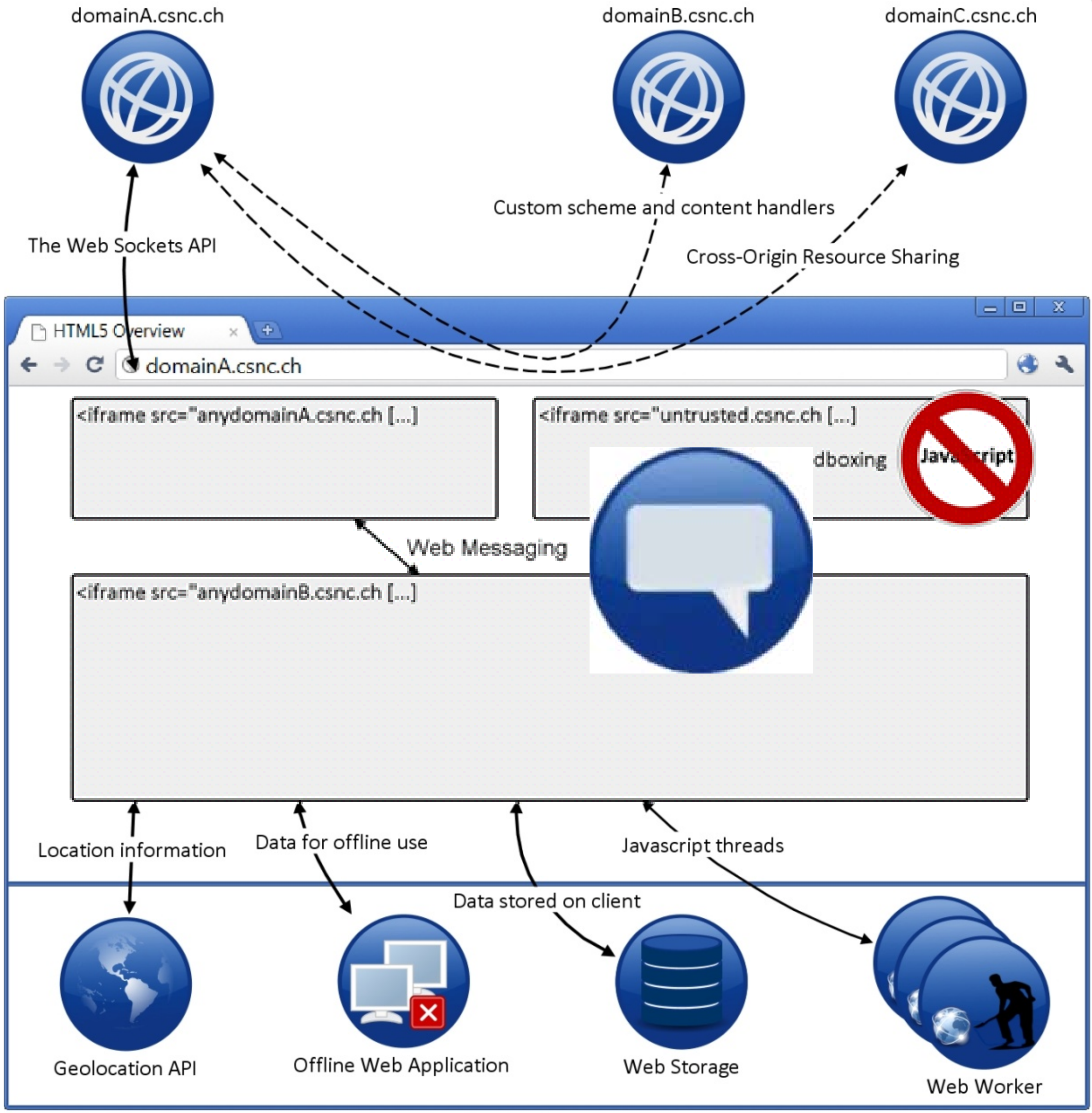
11: HTTP/1.1 200 OK
Login successful

User Training

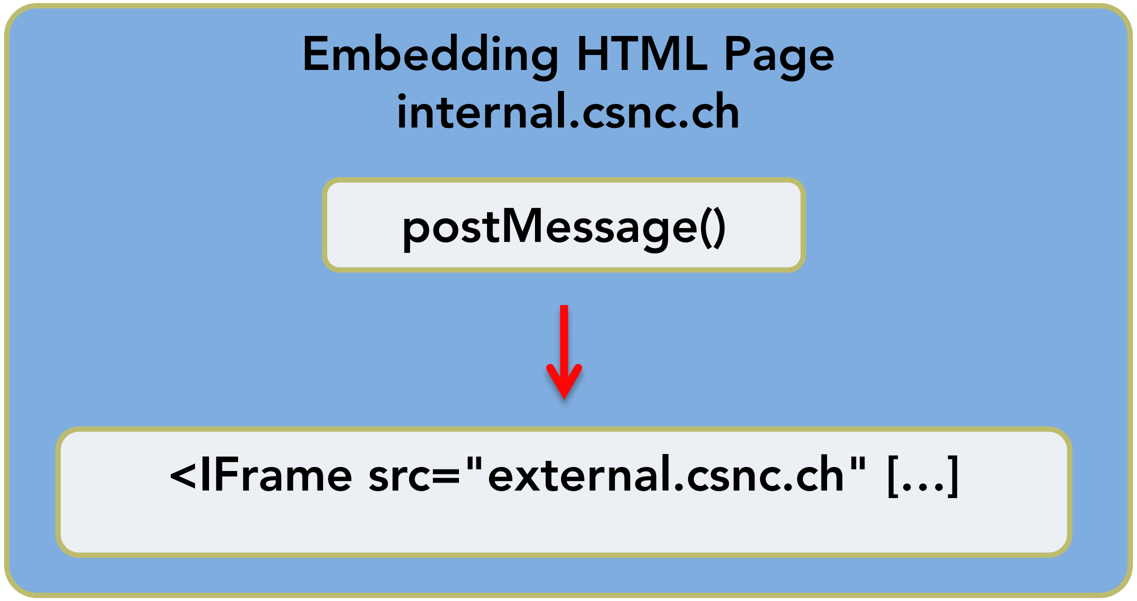
=> Do not accept caching of web applications!

=> Clear the cache including Local Storage and Offline Web Applications!

Web Messaging



Web Messaging



Embedding HTML Page
internal.csnc.ch

postMessage()

<IFrame src="external.csnc.ch" […]

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.

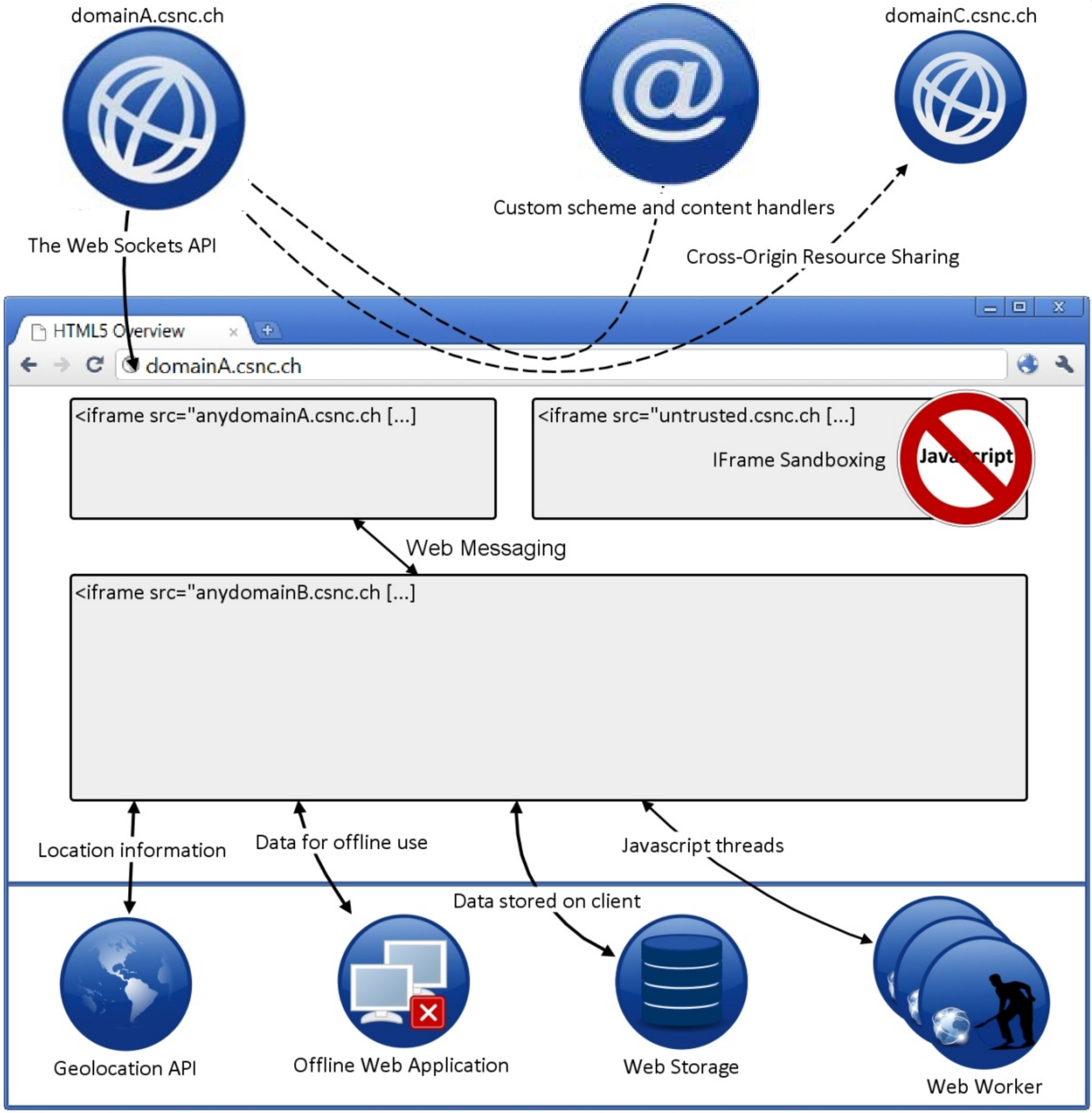
Countermeasures

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

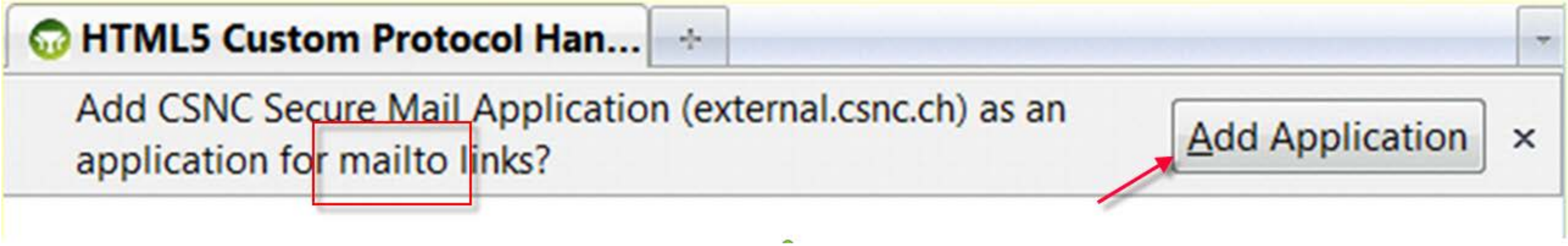
The receiving IFrame should not accept messages from any domain. E.g. `e.origin == "http://internal.csnc.ch"`

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



Add CSNC Secure Mail Application (external.csnc.ch) as an application for mailto links?

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

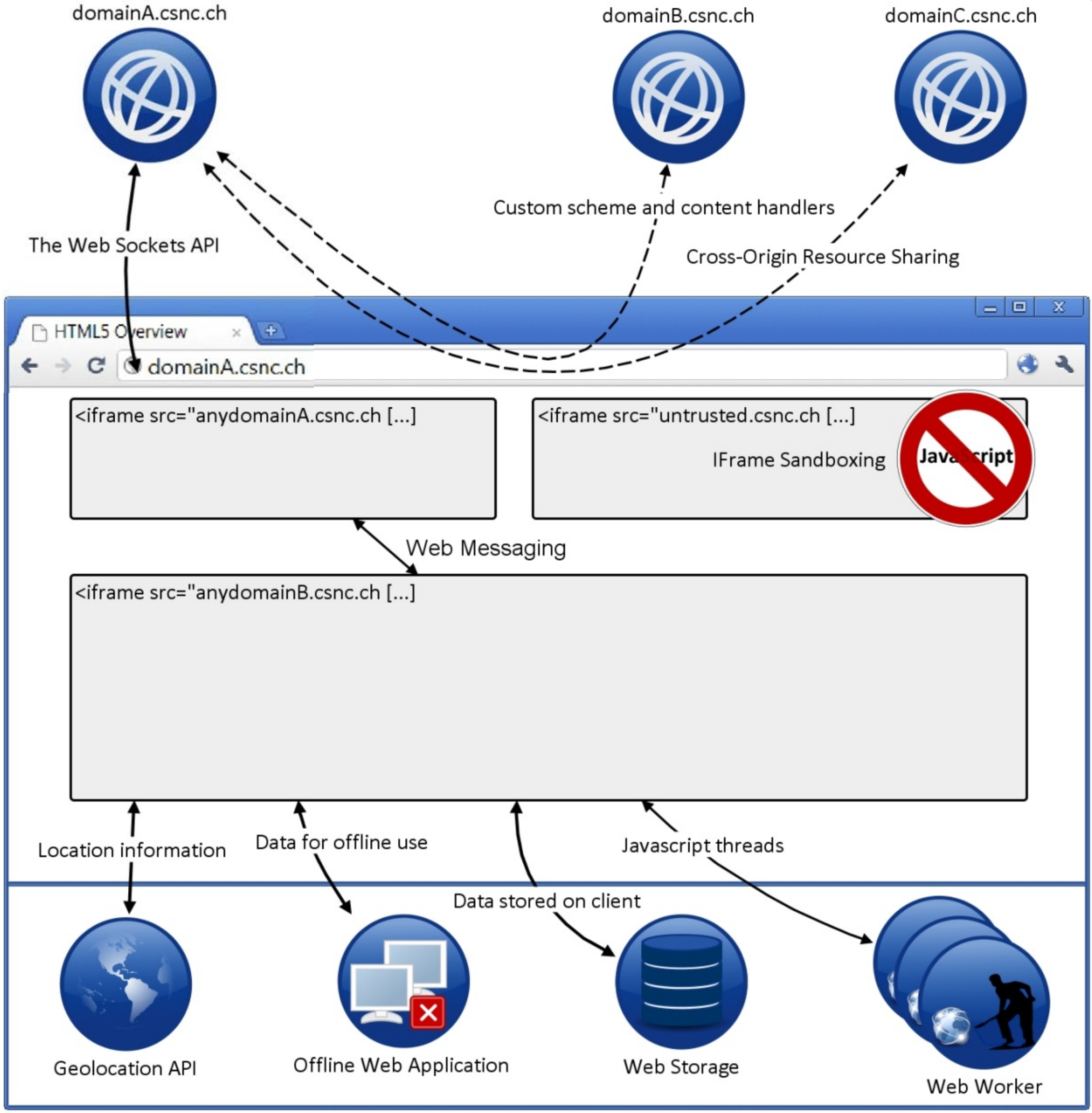
- Additional possibility to identify a user.
- Unique identifiers could be stored along with the protocol handler.

Countermeasures

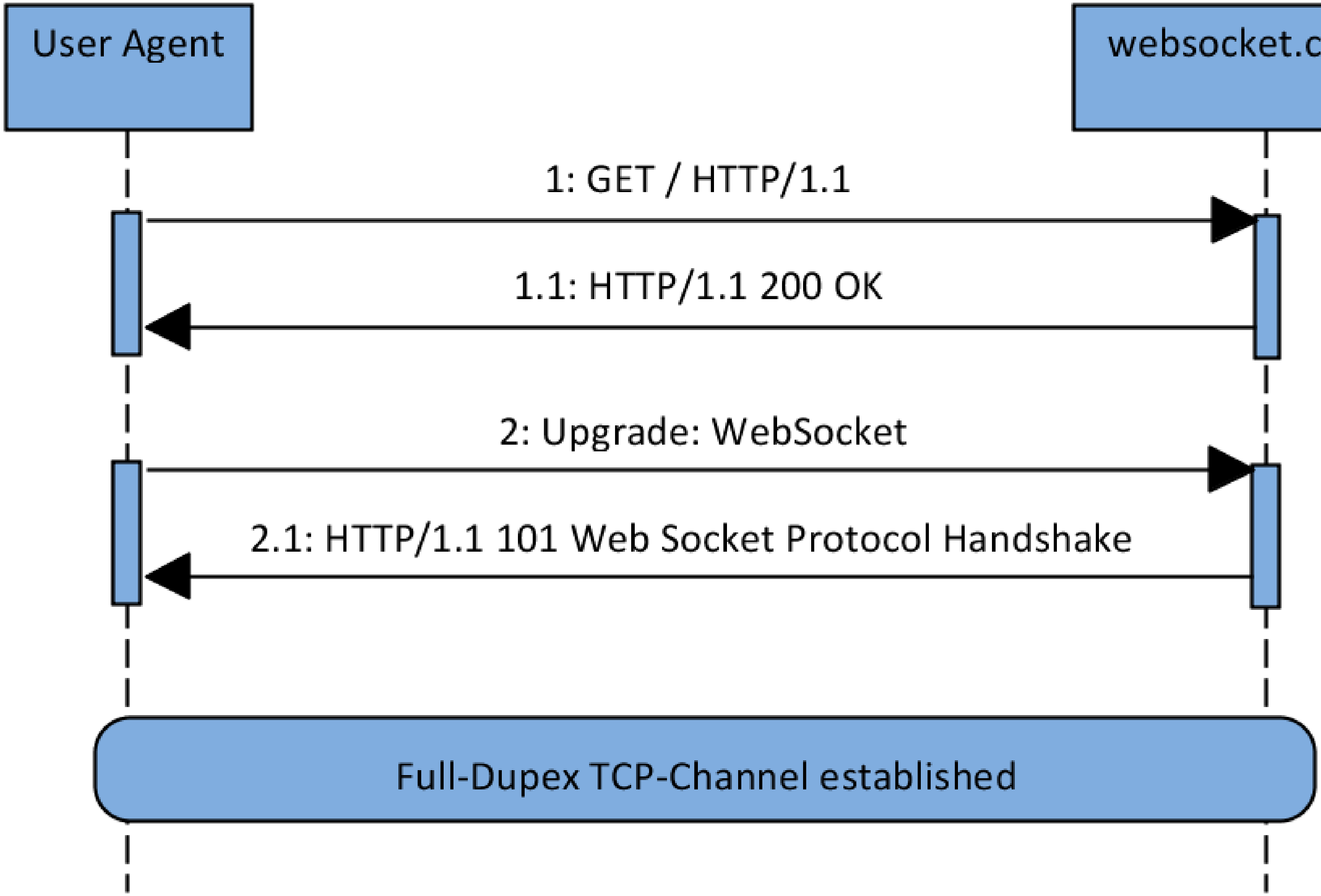
User Training

=> Do not accept registration of protocol handlers!

Web Sockets API



Web Sockets API



Web Sockets API – Vuln. & Threats

Cache Poisoning

- A misunderstanding proxy could lead to a cache poisoning vulnerability.
  → **Fixed** by introducing masking of the web socket data frames.

Scanning the internal network

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

Establishing a remote shell

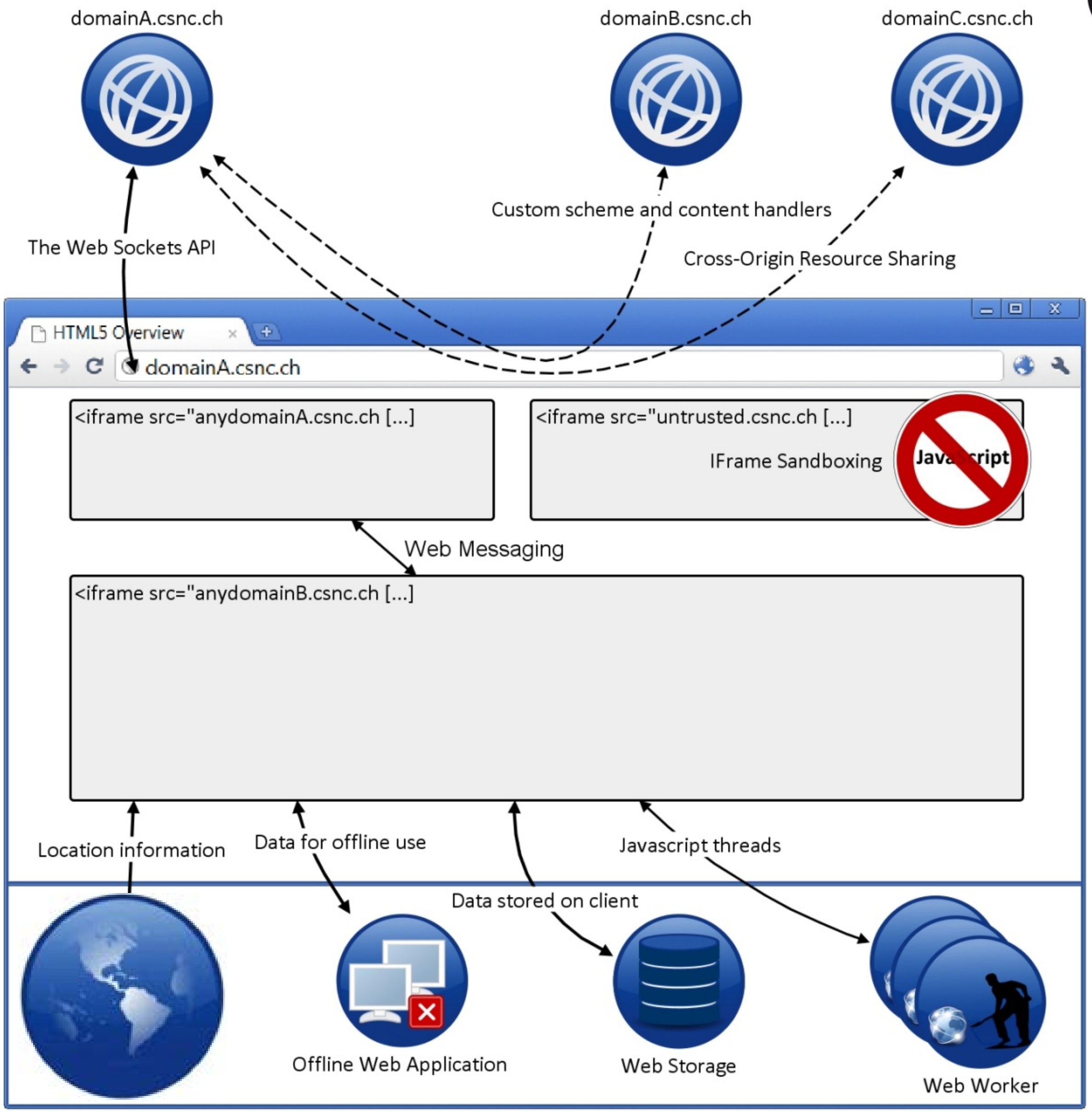
- Web Sockets can be used to establish a remote shell to a victim's browser.

Countermeasures

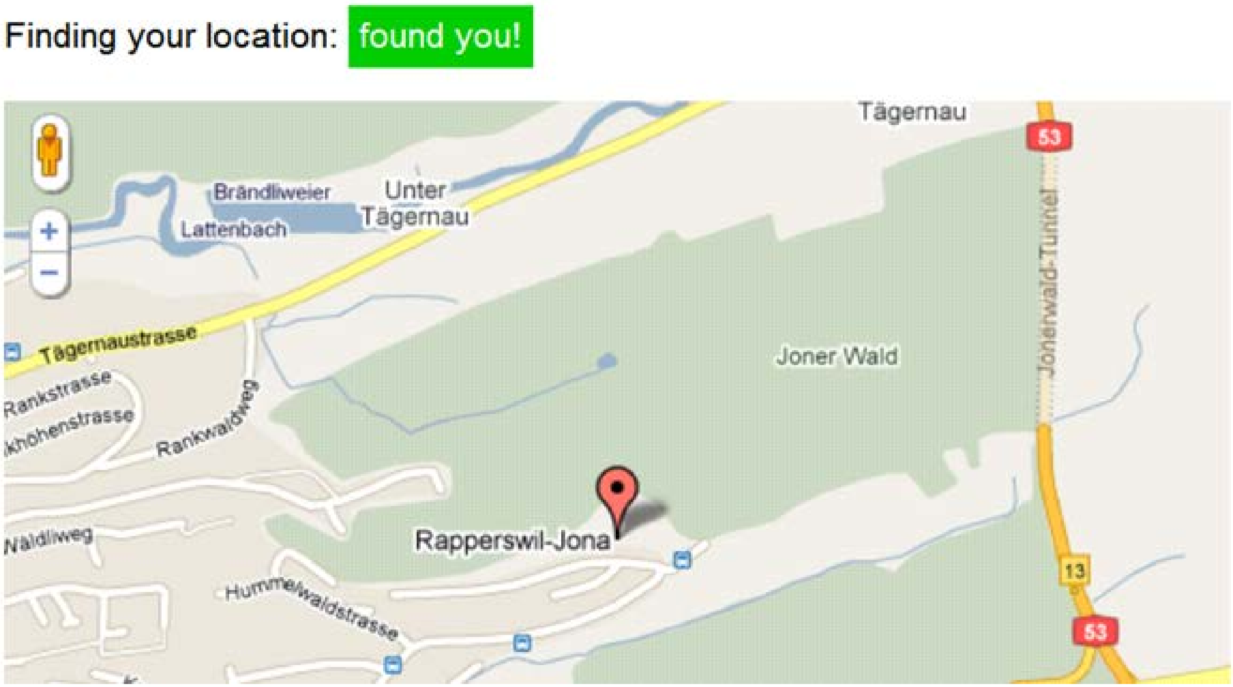
The risks of the Web Sockets API needs to be accepted.

The user could disable it in the browser.

Geolocation API



Geolocation API


Finding your location: found you!

User Tracking

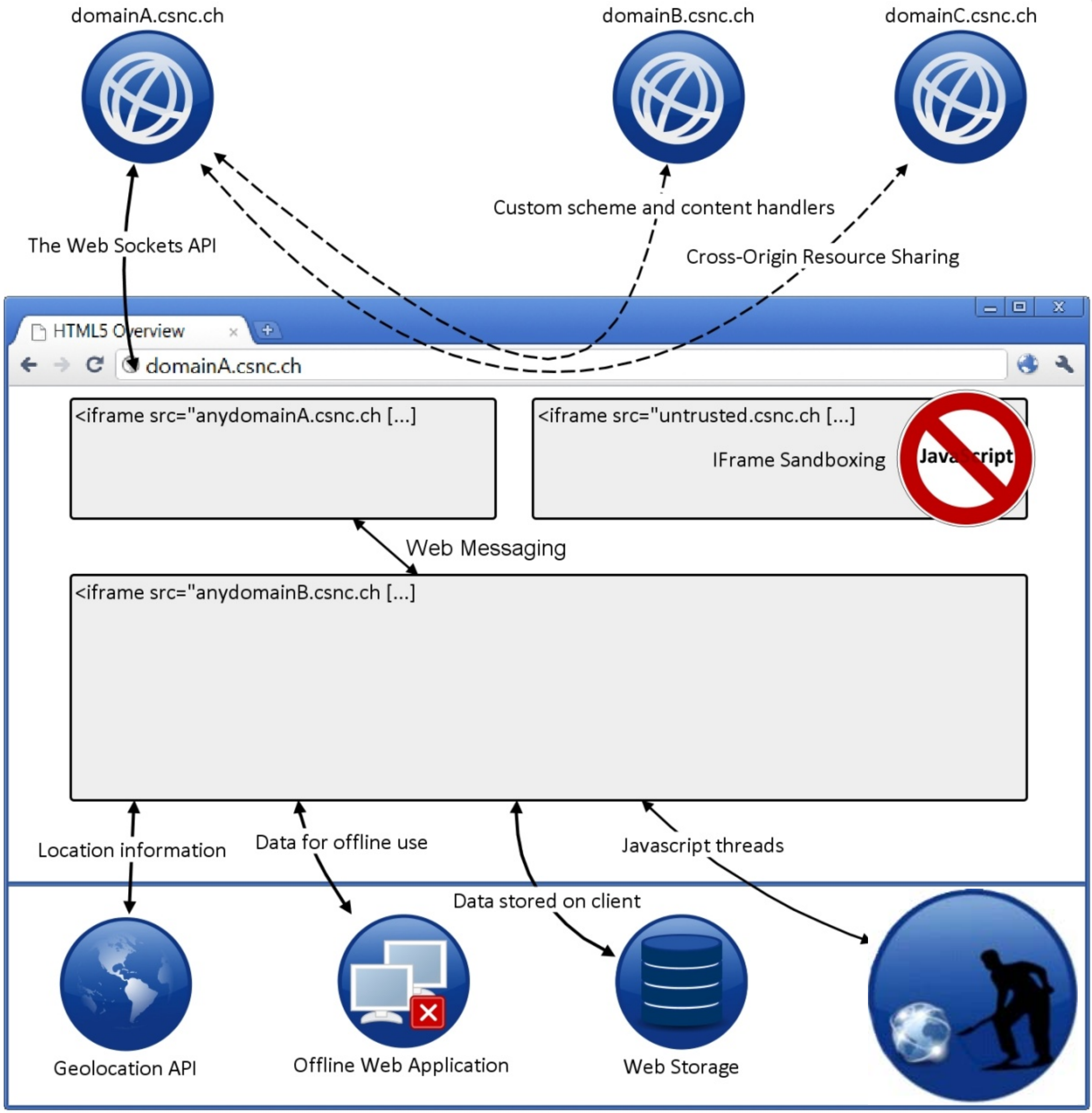
- ✦ User tracking based on the location of a user.
- ✦ If users are registered, their physical movement profile could be tracked.
- ✦ The anonymity of users could be broken.

Countermeasures

User Training

=> Do not accept to share location information!

Web Workers


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

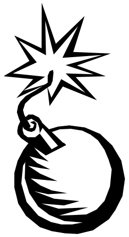
But they can be used indirectly for launching work intensive attacks without the user noticing it.

Worst Case Scenarios

Web Workers = *Feature!*

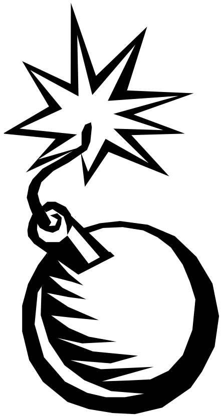
Cracking Hashes in JS Cloud *(DEMO).*

Web Workers + Cross-Origin Resource Sharing =



Powerful DDoS attacks.

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



Web-based Botnet.

Conclusion

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.

Not all issues can be mitigated through secure server-side implementation.

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-Site Scripting (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 IE 6

;)

DEMO – Exploiting Cross-Origin Resource Sharing

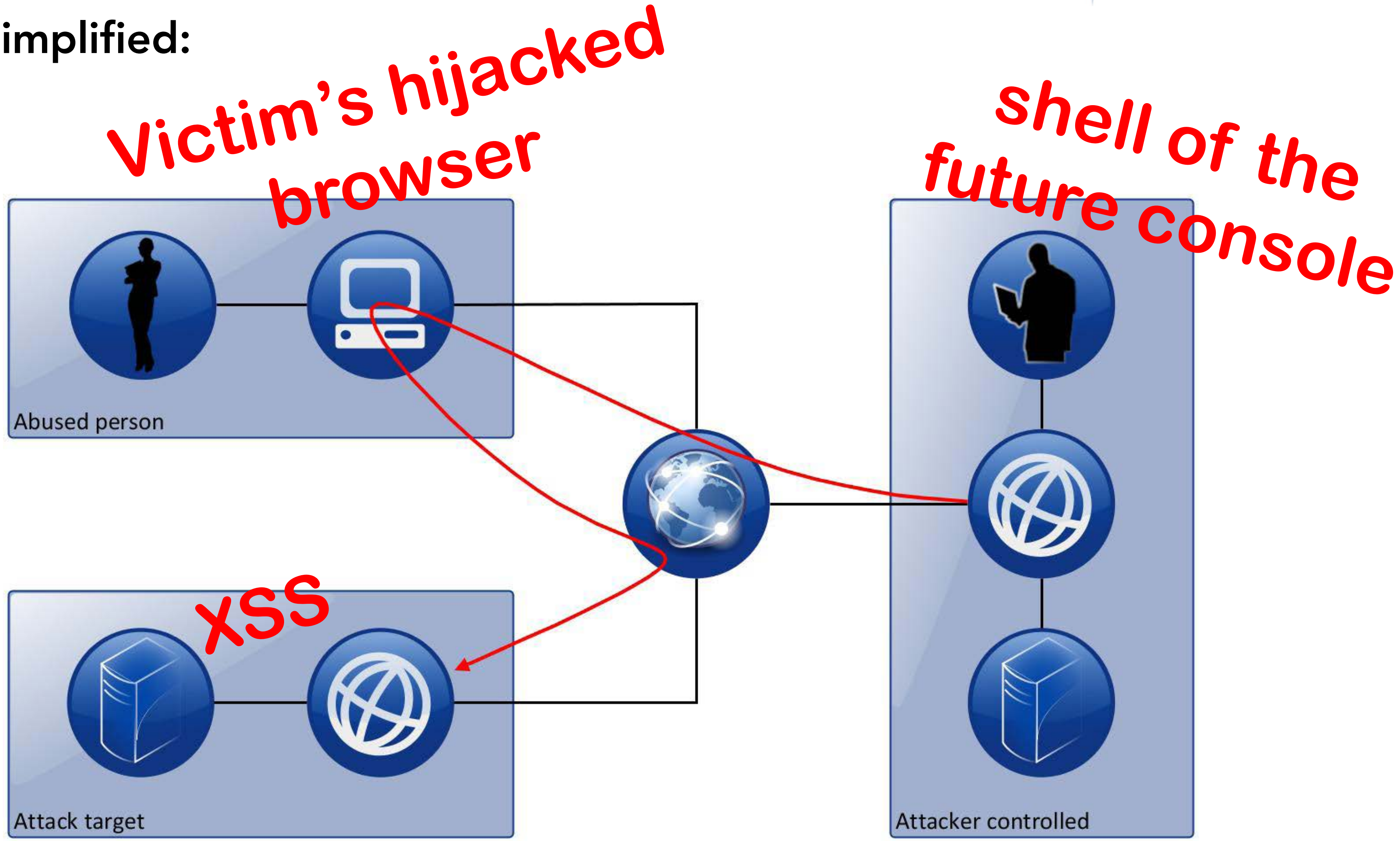
Shell of the Future

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

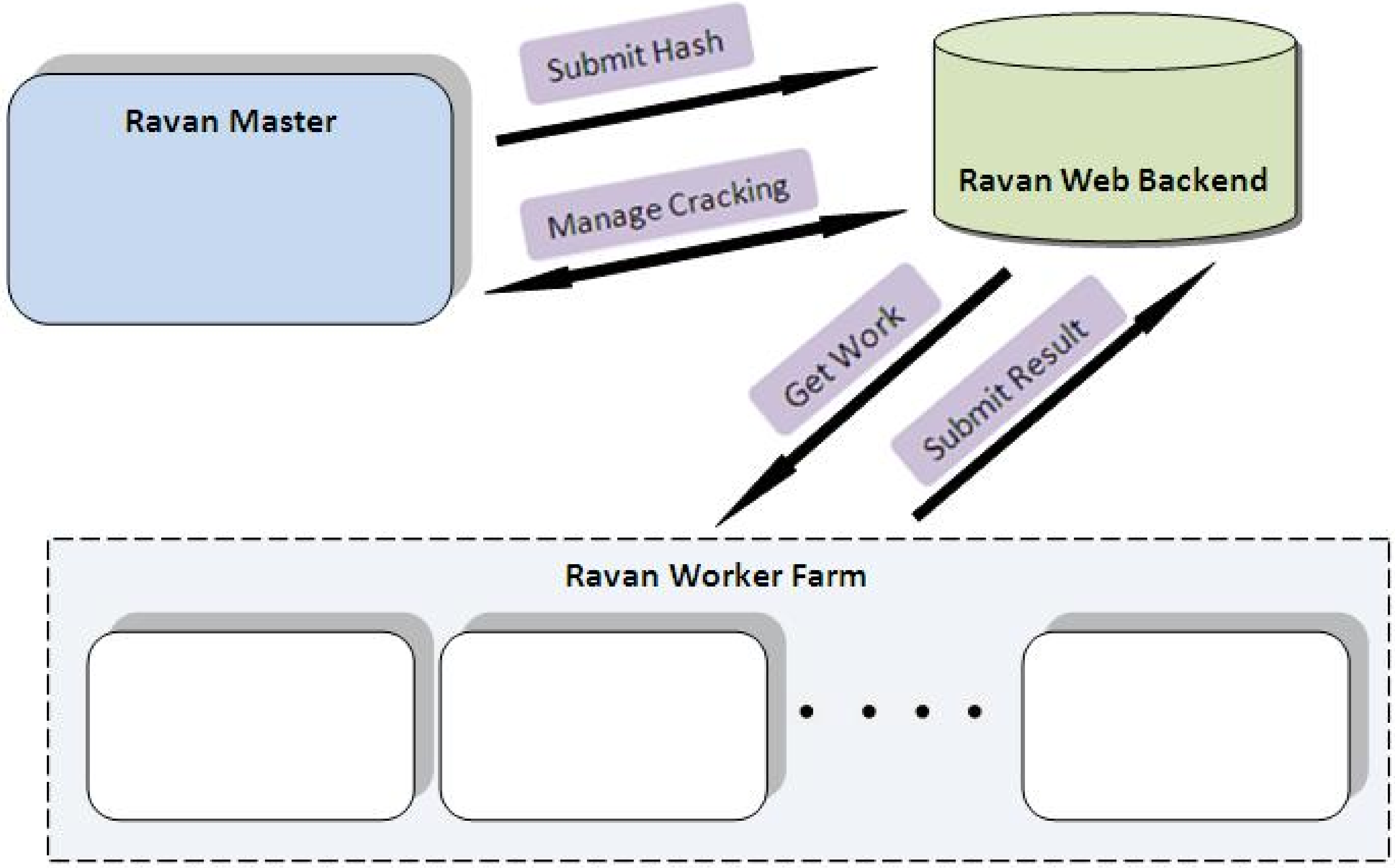
Ravan

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

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

14d6a3e0201f58bfe7c01e775973e80e

Quiz and Q&A

DEMO – Web Workers – Ravan

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

BREAK

Presentation Video Online: http://www.youtube.com/watch?v=Eju4e5mhEN0

Try HTML5 cases at home:
https://www.hacking-lab.com/sh/Gb5VF4q

References

- **Master Thesis „HTML 5 web security"**
  Michael Schmidt
  31 March 2011

- **Article „HTML5 web security"** *(extract of master thesis)*
  Michael Schmidt, Thomas Röthlisberger
  6 December 2011
  http://media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf

- **Attack and Defense Labs**
  Lavakumar Kuppan
  http://www.andlabs.org

- **A vocabulary and associated APIs for HTML and XHTML**
  W3C, HTML5 specification
  17 December 2012
  http://www.w3.org/TR/html5/