

Saarbrücken, 29th June 2016

Daniel Waxweiler

Supervisor:

Prof. Dr. Michael Backes

Prof. Dr. Antonio Krüger

Advisors:

Dr. Sascha Fahl

Yasemin Acar

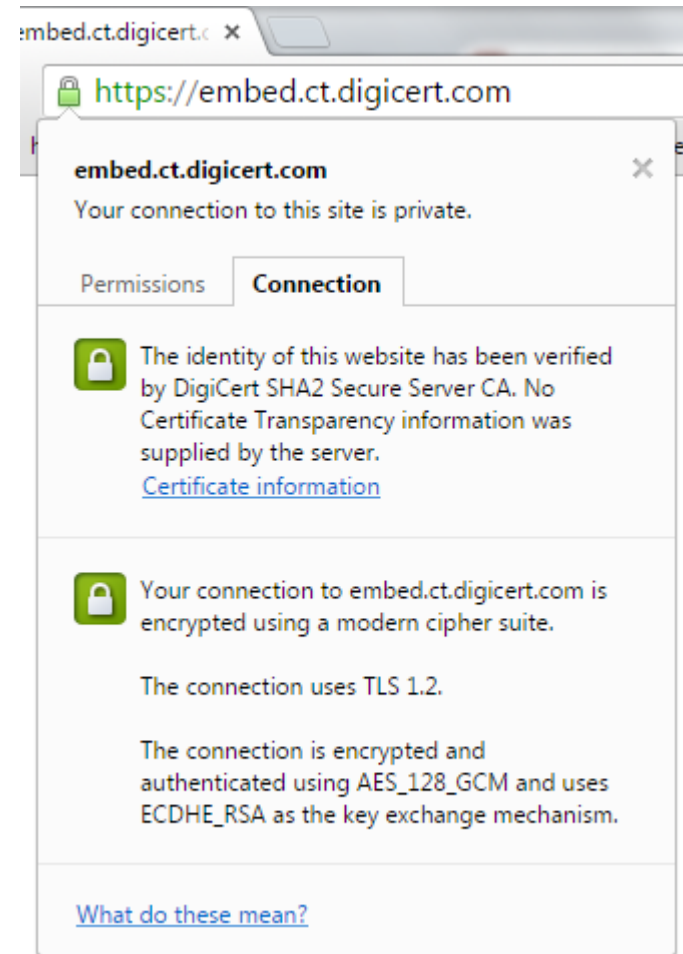
Christian Stransky

Saarland University
Master seminar

Making Chromium's Certificate Transparency integration more accessible

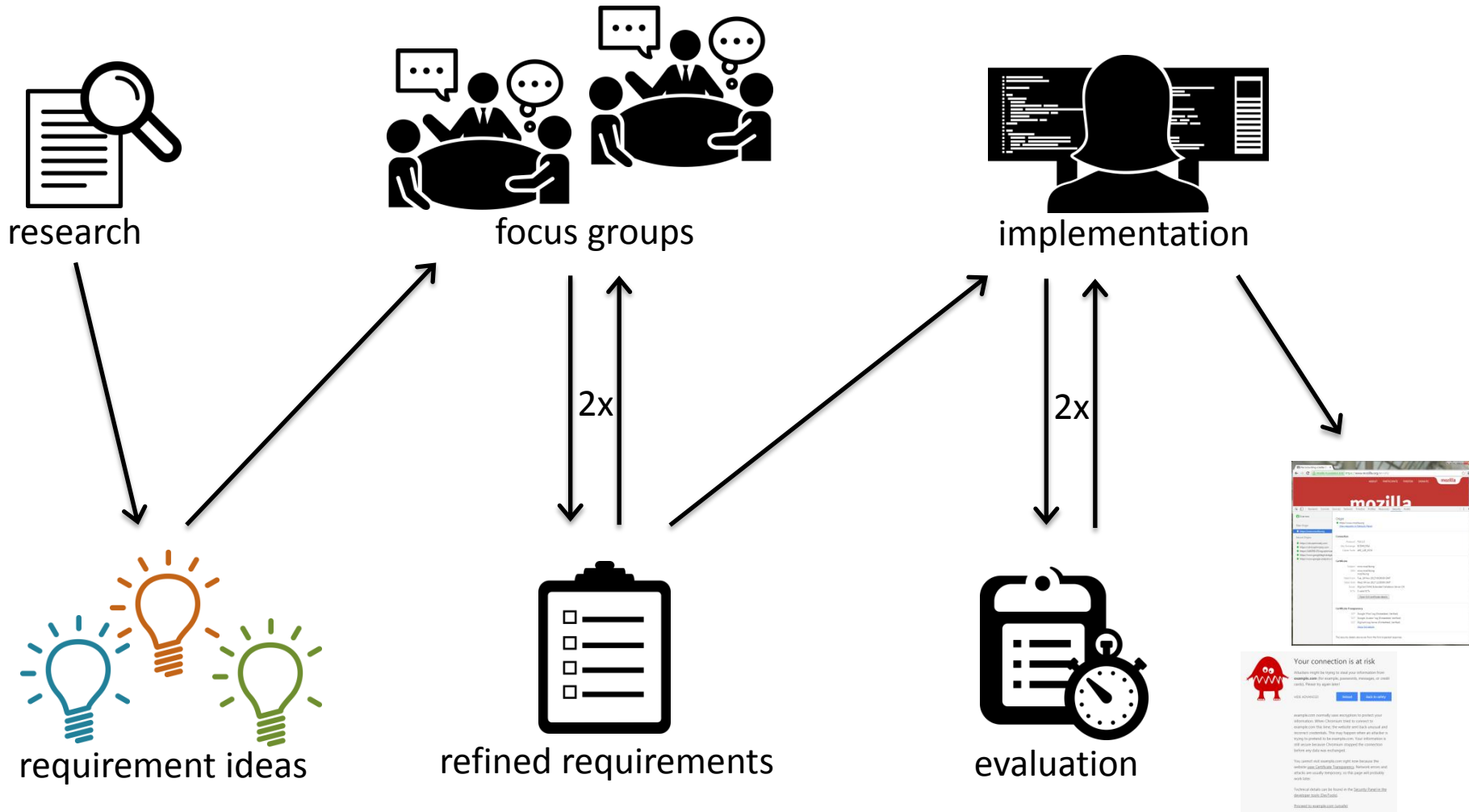
Goal of the thesis

- Improve Certificate Transparency integration in Chromium and Google Chrome
 - 60% of Internet users¹
- Discussions with and feedback from Google developers
- Code of some suggested features successfully integrated
 - job offer by Google



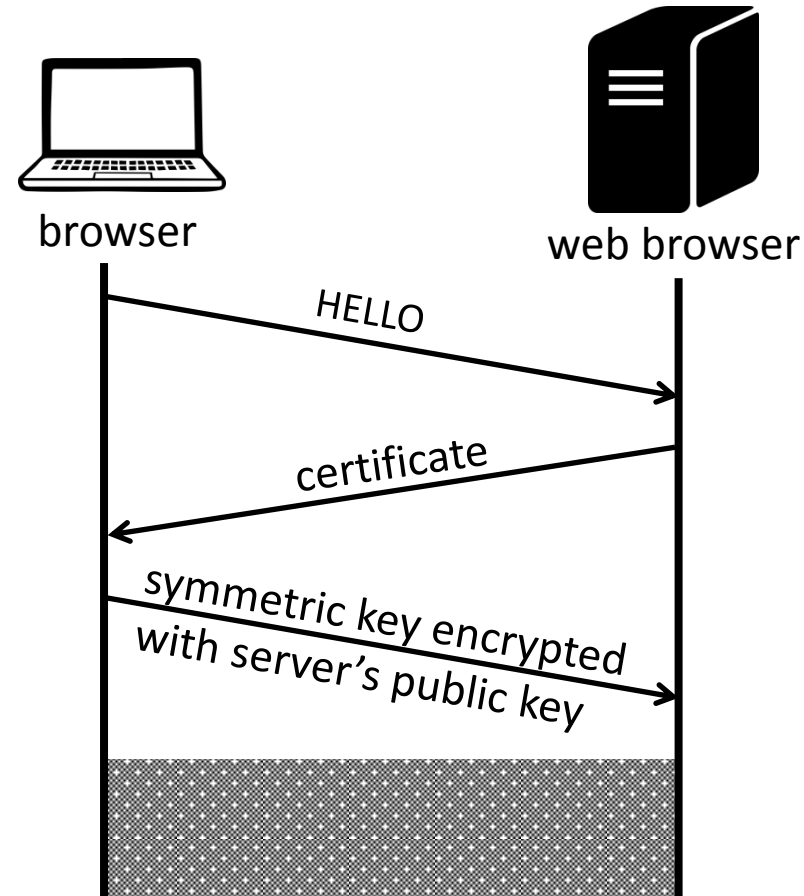
1: Desktop (PCs and laptops) browser market share in May 2016 according to *StatCounter Global Stats*

Iterative design process



SSL / TLS protocol

- Goal: secure communication between 2 entities
- Enhancing Transmission Control Protocol (TCP) on the application layer with
 - Confidentiality
 - Integrity
 - Authenticity
- Use of X.509 certificates



Public key certification

- Certificate of an entity
 - Public key of the entity
 - Globally unique information of the entity
e.g. domain name
 - Signature of a certificate authority (CA)
- Another entity can verify certificate.
- CA has to be trusted by both entities!



```
Certificate:
Data:
  Version: 1 (0x0)
  Serial Number: 7829 (0x1e95)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte
          OU=Certification Services Division,
          CN=Thawte Server CA/emailAddress=server-
Validity
  Not Before: Jul  9 16:04:02 1998 GMT
  Not After : Jul  9 16:04:02 1999 GMT
  Subject: C=US, ST=Maryland, L=Pasadena, O=Brent R
          OU=FreeSoft, CN=www.freesoft.org/emailA
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
  Modulus (1024 bit):
    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:1
    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:
    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:
    70:33:52:14:c9:ec:4f:91:51:70:39:de:
    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:
    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:
    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:
    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:
    e8:35:1c:9e:27:52:7e:41:8f
  Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
  93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:
  92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:
  ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:
  d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:
  0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:
  5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:c
  8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:
  68:9f
```

System failure example

Dutch CA



- Compromised
- At least 531 false certificates¹
- Used to conduct MITM attacks in Iran²
- Revoked only months later

1: <http://blog.gerv.net/2011/09/updated-diginotar-cn-list/>

2: <http://www.theguardian.com/technology/2011/aug/30/faked-web-certificate-iran-dissidents>

```
*.million.org  
*.android.com  
*.aol.com  
*.azadegi.com  
*.balatarin.com  
*.comodo.com  
*.digiCert.com  
*.globalsign.com  
*.google.com  
*.JanamFadayeRahbar.  
*.logmein.com  
*.microsoft.com  
*.mossad.gov.il  
*.mozilla.org  
*.RamzShekaneBozorg.  
*.SahebeDonyayeDigit.  
*.skype.com  
*.startssl.com  
*.thawte.com  
*.torproject.org  
*.walla.co.il  
*.windowsupdate.com
```

Public key infrastructure flaws

Certificates can be issued by CAs

- Being comprised
- By mistake
- Turning evil
- Being blackmailed

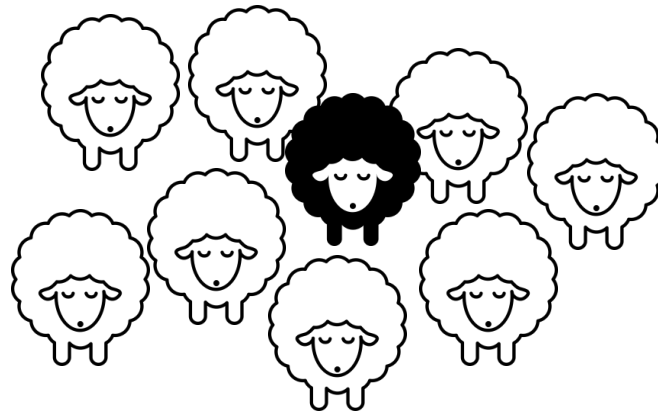


→ used to conduct MITM attacks

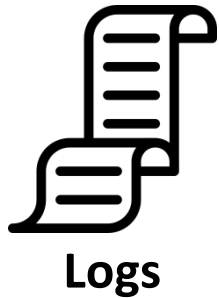
→ impossible to detect

Certificate Transparency

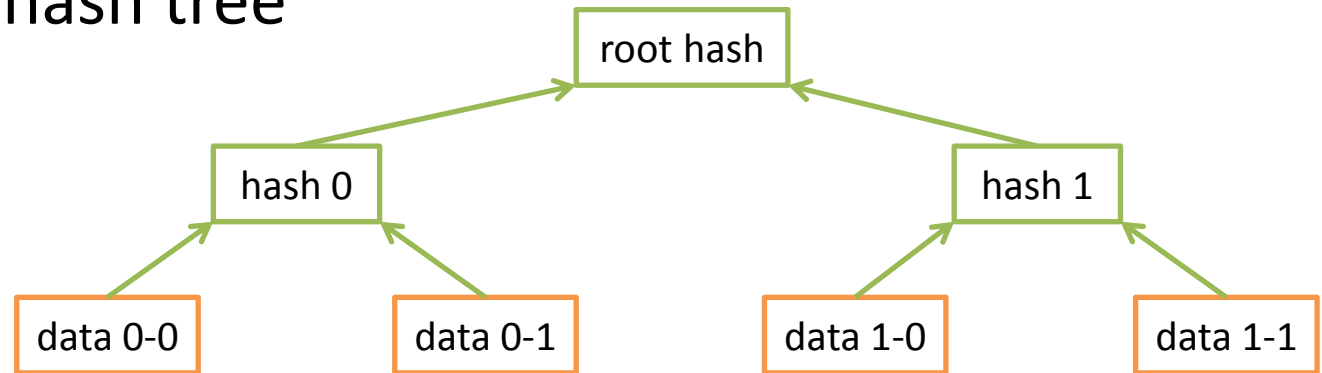
- Invented by Ben Laurie and Adam Langley working at Google
- Experimental Internet Engineering Task Force (IETF) standard
- Goal: detect false certificates issued by CAs in nearly real-time



Certificate Transparency



- Heart of the system
- Used cryptographic mechanism: Merkle hash tree



- Properties
 - Append-only records of certificates
 - Cryptographically assured
 - Publicly auditable



Certificate Transparency



Logs

- Act as clients to the log servers
- Regularly copy everything new
- Constantly verify logs
- Can act as backup read-only logs



Monitors



Auditors

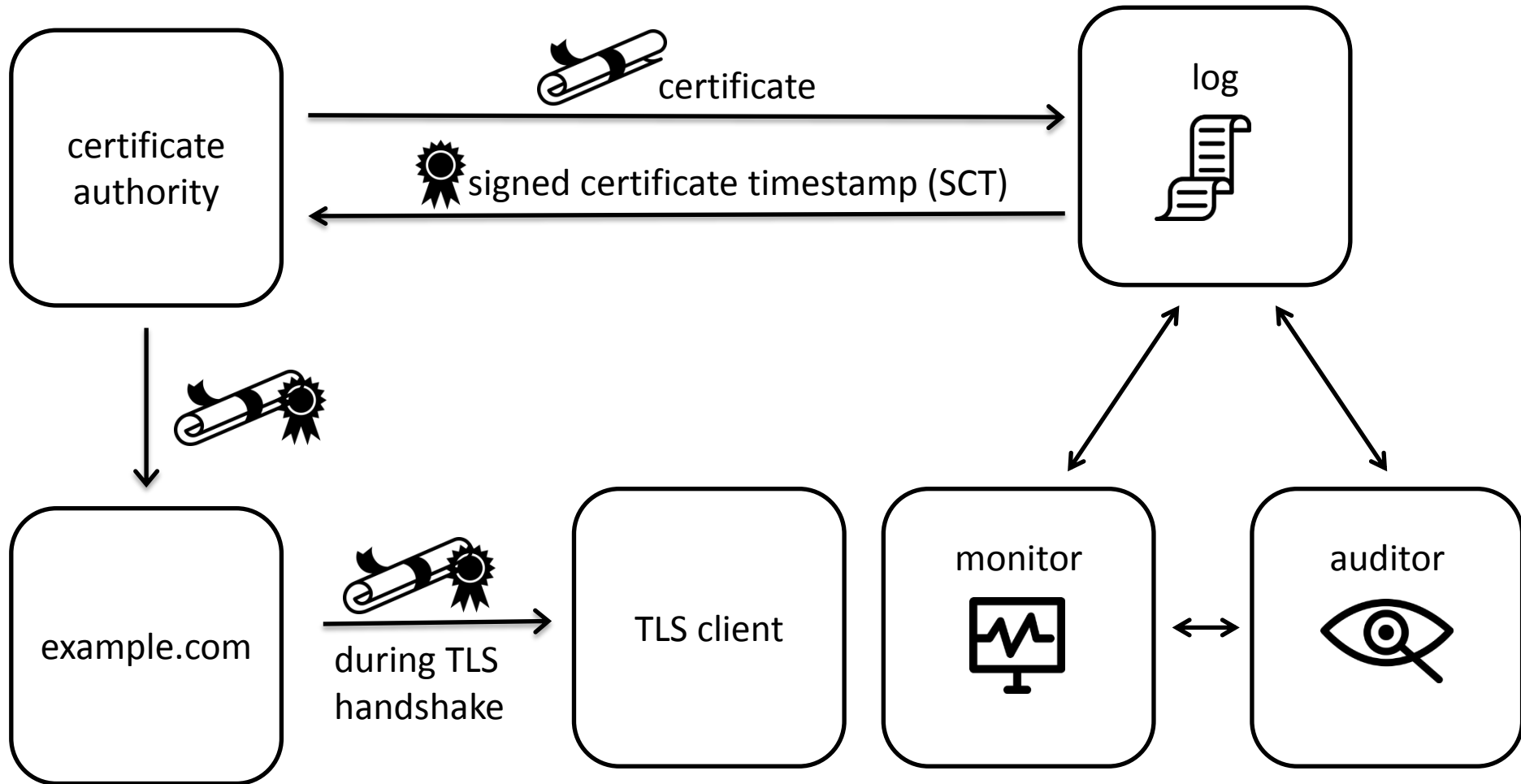
Certificate Transparency



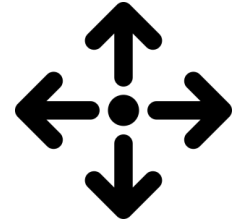
- Act as clients to the log and monitor servers
- Verify logs
- Verify a particular certificate
- Can be integrated into end client applications, e.g. web browser



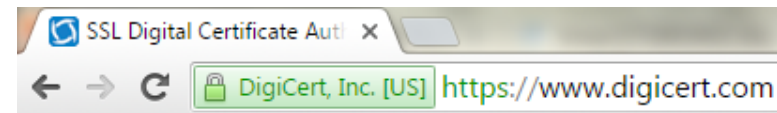
Certificate Transparency



Certificate Transparency

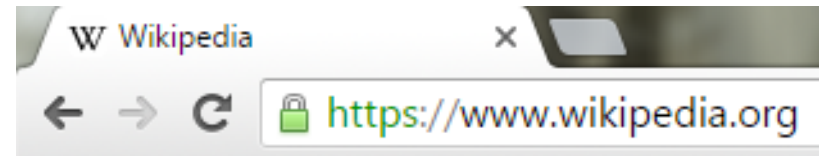


- 14 logs operated by *Google, Symantec, Izenpe, Certly* and many more
- Browsers
 - Google Chrome
 - based on open-source web browser Chromium
 - obligatory for EV certificates
 - Mozilla Firefox: no schedule, but some code changes in the pipeline
 - No announcement from Microsoft and Apple yet



First ideas

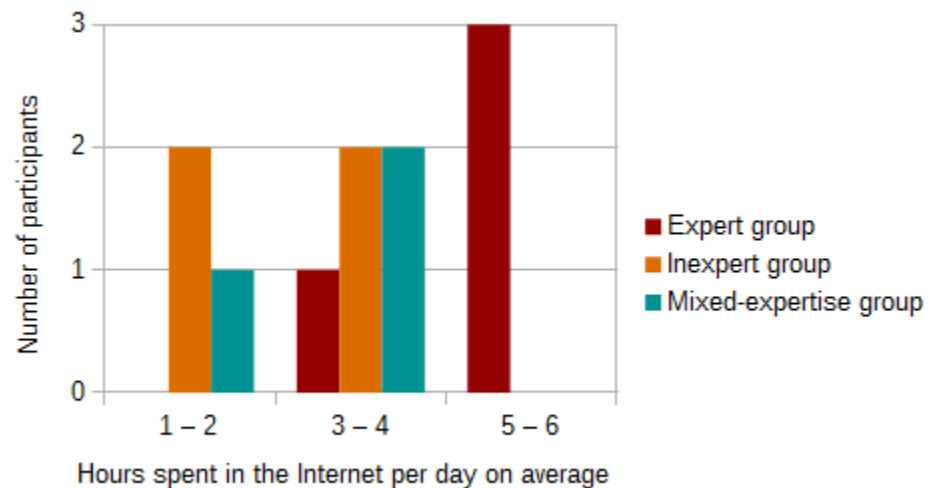
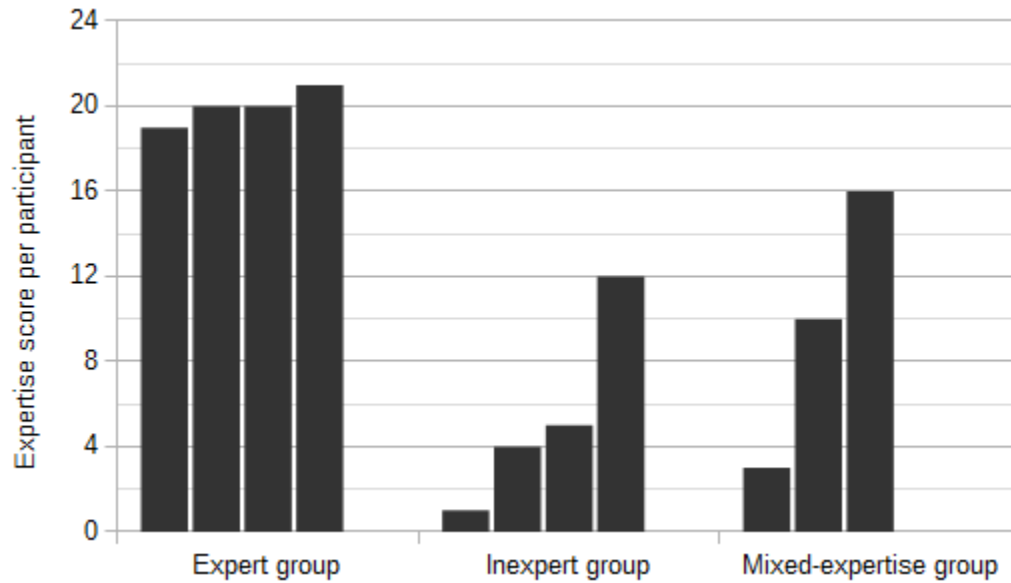
- Show an interruptive warning
- Adapt lock icon and https indicator in location bar
- Adjust website popup
- Add a dialog with SCT(s) details
e.g. name of log and issuance time



Exploration focus groups

- Goal: collect users' ideas of how to make the CT information usable, accessible and understandable
- Online pre-questionnaire
 - Requirement: use Google Chrome or Chromium
 - 10 of 11 participants: students
- Expertise score = sum of ratings on the 5-point Likert scale to statements, e.g.
 - I have a solid level of Internet experience.
 - I know what a digital certificate is.
 - I know how to install a digital certificate on a web server.

Exploration focus groups



Requirements

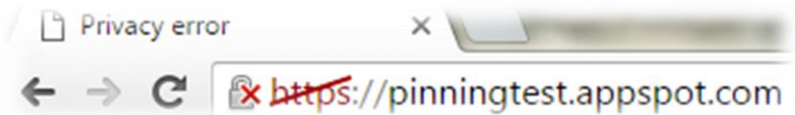
- All CT checks passed

→ only adaption of passive indicators



- One CT check failed

→ adaption of passive indicators & error page



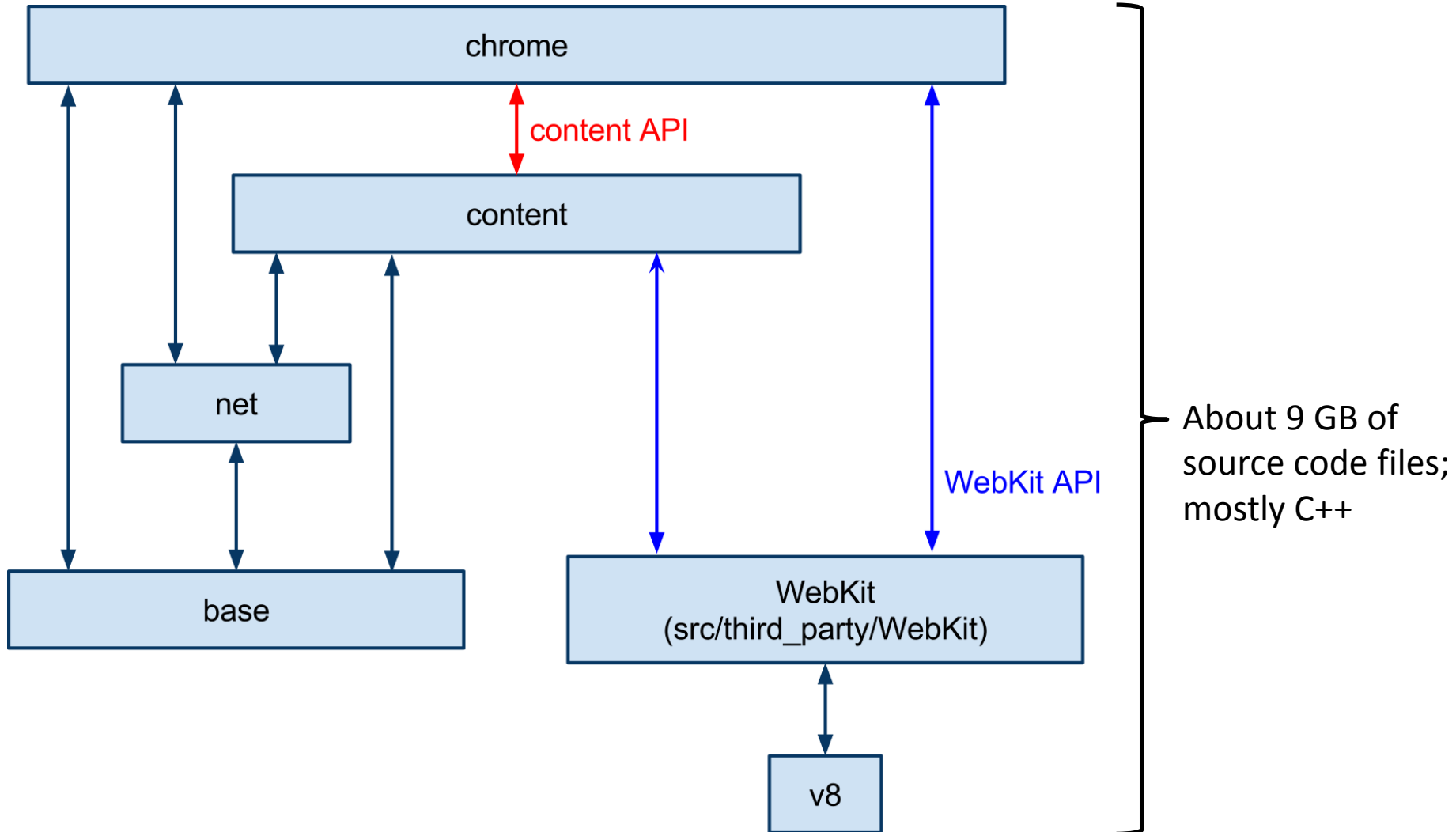
- More information for experts

– Setting to enable a button on error page to continue to the possibly false website

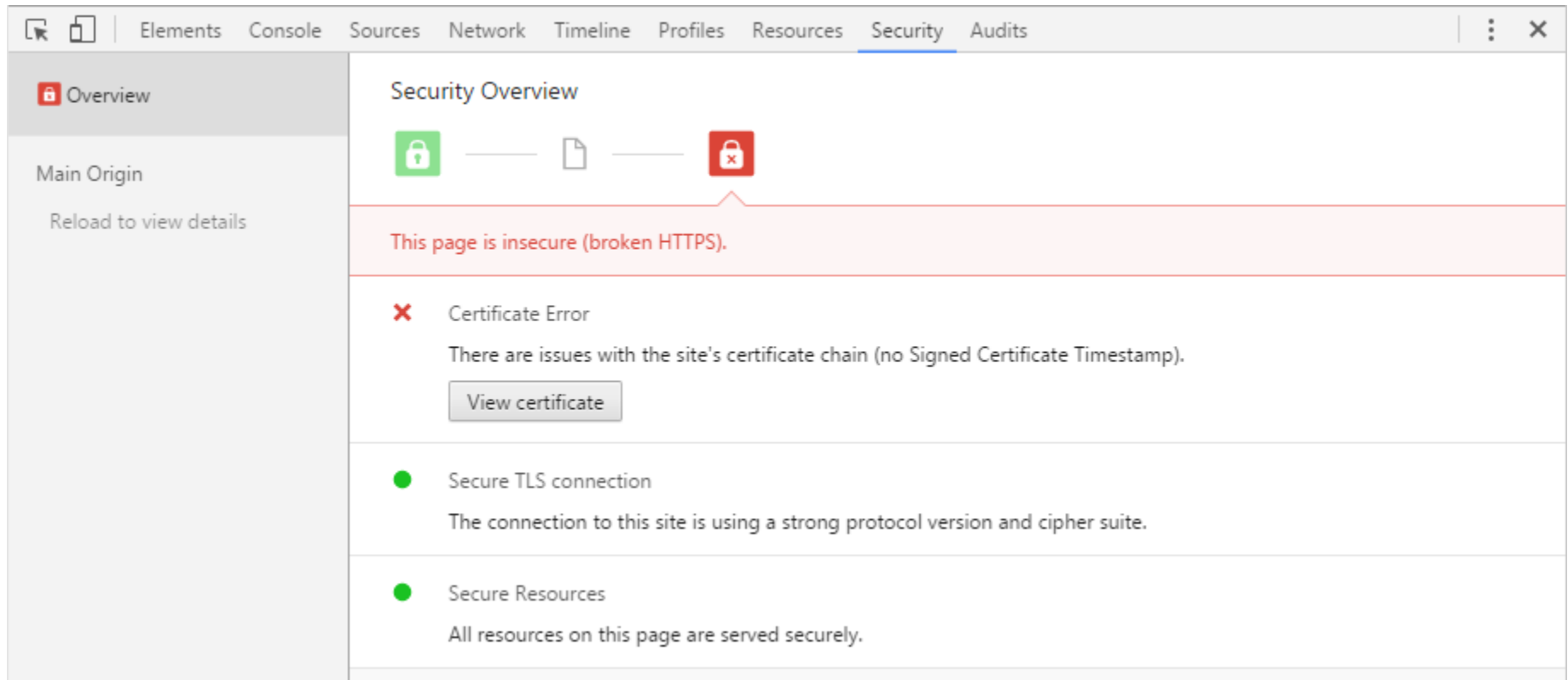
– SCT details in Security Panel in DevTools



Implementation



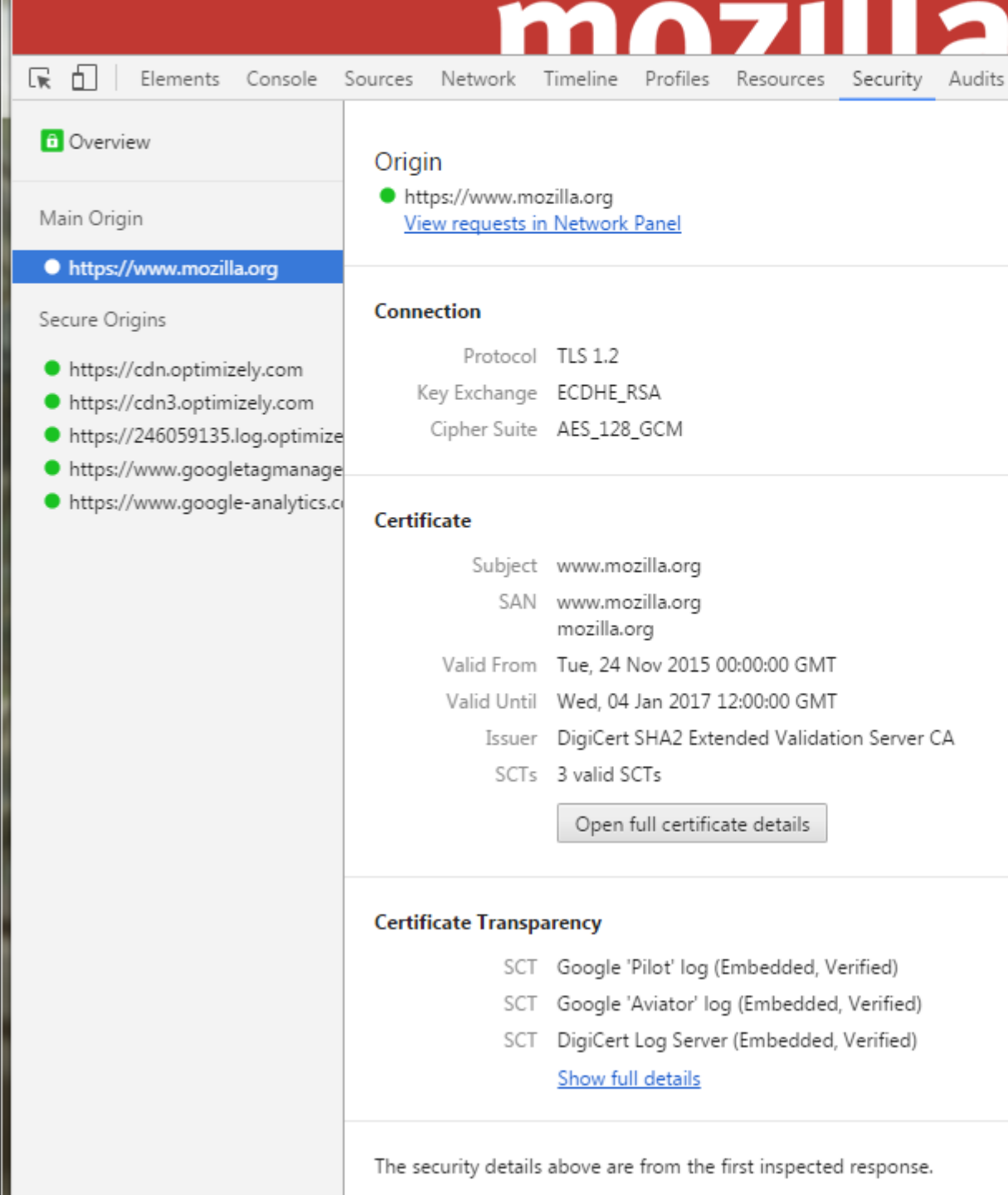
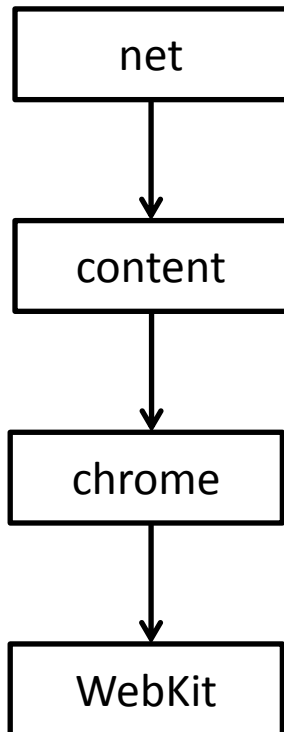
DevTools



52 changed lines

DevTools

Piped through the different modules



Overview

Main Origin

https://www.mozilla.org

Secure Origins

- https://cdn.optimizely.com
- https://cdn3.optimizely.com
- https://246059135.log.optimizely.com
- https://www.googletagmanager.com
- https://www.google-analytics.com

SCTs 3 valid SCTs

Open full certificate details

Certificate Transparency

Log Name Google 'Pilot' log

Log ID A4 B9 09 90 B4 18 58 14 87 BB 13 A2 CC 67 70 0A 3C 35 98 04 F9 1B DF B8 E3 77 CD 0E C8 0D DC 10

Validation Status Verified

Origin Embedded

Issued At Tue, 24 Nov 2015 04:10:02 GMT

Version 1

Hash Algorithm SHA-256

Sign Algorithm ECDSA

Signature Data 30 46 02 21 00 98 A9 69 0D E6 B0 9A D9 61 47 7E 4A 6A 80 B3 AA A5 93 18 EF 88 63 F2 ED B5 AA 72 ED 4C DB 71 21 02 21 00 F6 86 A3 83 4D 83 53 AB 26 AE 3F 2D 28 D3 22 AB E3 C9 86 A3 8B A9 91 AE 59 85 48 C7 FF 15 49 28

Log Name Google 'Aviator' log

Log ID 68 F6 98 F8 1F 64 82 BE 3A 8C EE B9 28 1D 4C FC 71 51 5D 67 93 D4 44 D1 0A 67 AC BB 4F 4F FB C4

Validation Status Verified

Origin Embedded

Issued At Tue, 24 Nov 2015 04:10:02 GMT

Version 1

Hash Algorithm SHA-256

Sign Algorithm ECDSA

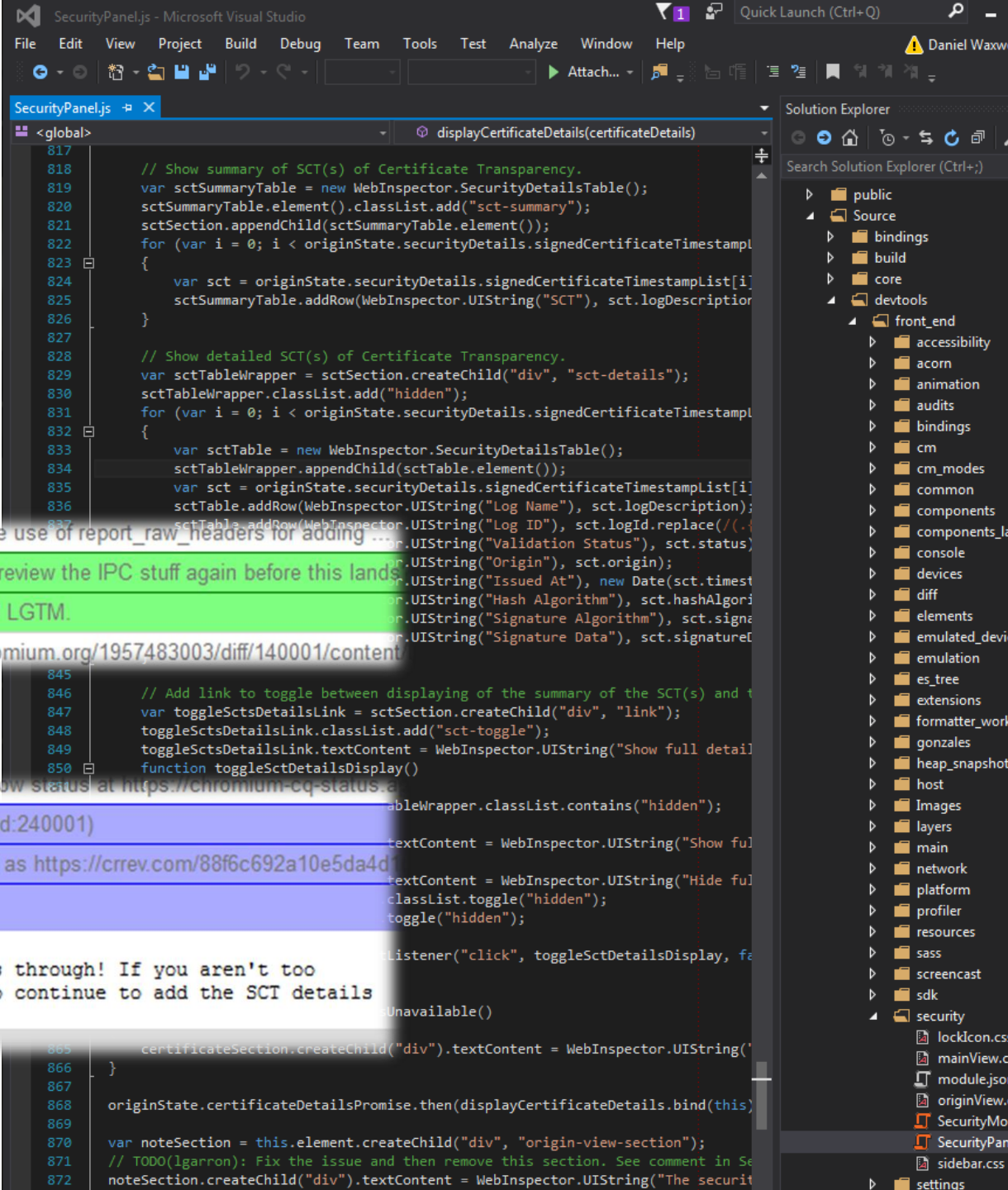
Signature Data 30 44 02 20 0B 91 93 5D 98 61 78 B8 00 17 68 AE C1 CA 0B 24 D4 46 8F E1 E0 0F D5 A2 FD 18 7E 05 B9 2F 4E 0F 02 20 51 98 7C 10 2C 3F D1 A8 8B 7E 7D 7A 25 8C 5F 2C E7 79 B5 3C 49 21 B7 28 6B 0D A0 AE 8D D0 21 E9

Log Name DigiCert Log Server

Log ID 56 14 06 9A 2F D7 C2 EC D3 F5 E1 BD 44 B2 3E C7 46 76 B9 BC 99 11 5C C0 EF 94 98 55 D6 89 D0 DD

DevTools

931 changed and contributed lines



me I have fixed the latest issues, such as commenting the use of report_raw_headers for adding

Charlie Reis Thanks! content/ LGTM. @palmer, can you review the IPC stuff again before this lands

palmer Yes, I was in the process of re-reviewing this. Still LGTM.

me Nice! Let's run the tests again. <https://codereview.chromium.org/1957483003/diff/140001/content>

commit-bot: I haz the power CQ is trying da patch. Follow status at <https://chromium-cq-status.a>

commit-bot: I haz the power Committed patchset #13 (id:240001)

commit-bot: I haz the power Patchset 13 (id:??) landed as <https://crrev.com/88f6c692a10e5da4d>

estark

Message was sent while issue was closed.

Daniel: nice job, thanks so much for seeing this through! If you aren't too burnt out from us annoying reviewers and want to continue to add the SCT details in devtools, that would be awesome. :)

[Reply](#)

Error page



Your connection is at risk

Attackers might be trying to steal your information from **example.com** (for example, passwords, messages, or credit cards). Please try again later!

HIDE ADVANCED

Reload

Back to safety

example.com normally uses encryption to protect your information. When Chromium tried to connect to example.com this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be example.com. Your information is still secure because Chromium stopped the connection before any data was exchanged.

You cannot visit example.com right now because the website uses Certificate Transparency. Network errors and attacks are usually temporary, so this page will probably work later.

Ask where to save each file before downloading

HTTPS/SSL

Manage certificates...

Show option to proceed through Certificate Transparency error pages

Google Cloud Print

Set up or manage printers in Google Cloud Print. [Learn more](#)

Manage

Error page

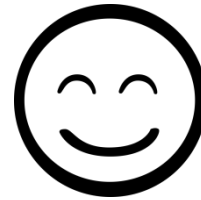
1843 lines
changed

```
...>git diff --stat 7175614caf3be7fa22ce4a8f6
...d2f63014182bcdade7752b1fb4
...erated_resources.grd          | 5 +
.../chrome_content_browser_client.cc | 5 +-
.../chrome_content_browser_client.h | 3 +-
...als/security_interstitial_page.cc | 26 +-
...als/security_interstitial_page.h | 7 +-
.../predictors/resource_prefetcher.cc | 7 +
.../predictors/resource_prefetcher.h | 3 +
.../profiles/profile.cc           | 1 +
...sources/options/browser_options.html | 23 +-
.../ssl/ct_blocking_page.cc       | 231 ++++++
.../ssl/ct_blocking_page.h        | 96 +++++
.../ssl/ssl_error_handler.cc      | 40 +-
.../ssl/ssl_error_handler.h       | 8 +-
...nterstitials/interstitial_ui.cc | 30 ++
...ptions/browser_options_handler.cc | 1 +
...rowser.gypi                   | 4 +
...pref_names.cc                 | 4 +
...pref_names.h                  | 1 +
...r/security_filter_peer.cc      | 8 +
...nterstitials_resources.grdp     | 3 +-
...urity_interstitials.gypi       | 2 +
...urity_interstitials/core/BUILD.gn | 2 +
...sources/images/monster-license.txt | 1 +
...er/resources/images/monster.png | Bin 0 -> 1
...erated_resources.grd          | 5 +
.../chrome_content_browser_client.cc | 5 +-
.../chrome_content_browser_client.h | 3 +-
...als/security_interstitial_page.cc | 26 +-
...als/security_interstitial_page.h | 7 +-
.../predictors/resource_prefetcher.cc | 7 +
.../predictors/resource_prefetcher.h | 3 +
.../profiles/profile.cc           | 1 +
...sources/options/browser_options.html | 23 +-
.../ssl/ct_blocking_page.cc       | 231 ++++++
.../ssl/ct_blocking_page.h        | 96 +++++
.../ssl/ssl_error_handler.cc      | 40 +-
.../ssl/ssl_error_handler.h       | 8 +-
...nterstitials/interstitial_ui.cc | 30 ++
...ptions/browser_options_handler.cc | 1 +
```

The screenshot shows the Microsoft Visual Studio IDE. The main window displays the source code for `ct_error_ui.cc`. The code includes a copyright notice, several `#include` statements for headers like `components/security_interstitials/core/ct_error_ui.h`, `base/i18n/time_formatting.h`, `chrome/browser/devtools/devtools_toggle_action.h`, `chrome/browser/devtools/devtools_window.h`, `components/security_interstitials/core/common_string_util.h`, `components/ssl_errors/error_classification.h`, `components/ssl_errors/error_info.h`, `grit/components_strings.h`, and `ui/base/i10n/i10n_util.h`. It also defines a namespace `security_interstitials` and a class `CTErrorUI` with a constructor and a `PopulateStringsForHTML` method. The Solution Explorer on the right shows the project structure, including folders like `page_load_metrics`, `pairing`, `password_manager`, `plugins`, `policy`, `power`, `precache`, `prefs`, `pref_registry`, `printing`, `profile_metrics`, `proximity_auth`, `proxy_config`, `query_parser`, `quirks`, `rappor`, `renderer_context_n`, `resources`, `rlz`, `safe_browsing_db`, `safe_json`, `scheduler`, `search`, `search_engines`, `search_provider_lo`, `security_interstitial`, and `core`.

Walk-through

- Goal: get some quick feedback
- Demonstration of the new features to 4 people
- Results
 - Mainly positive reactions
 - Found a typo
 - A few complained that it is not easy to bypass the error page.
- Implications
 - Fixed typo
 - No design changes as it should not be made too easy to proceed through an error page.



Online questionnaire

- Goal: get more detailed feedback
- Tasks:

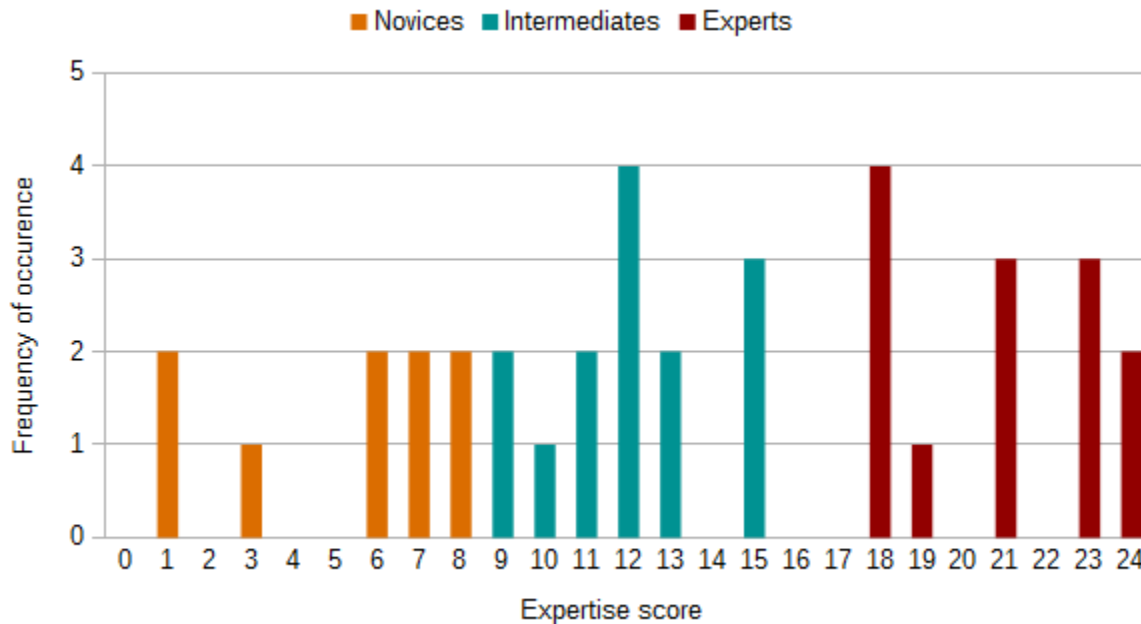
Task	Target group	Version of Google Chrome	CT information
A	Experts & inexperts	Current	Valid
B	Experts & inexperts	Current	Invalid
C	Inexperts	New	Valid
D	Inexperts	New	Invalid
E	Experts	New	Valid
F	Experts	New	Invalid

- Pilot study
 - Think-aloud technique
 - 4 participants
 - Discovered several comprehension and navigation issues

Online questionnaire

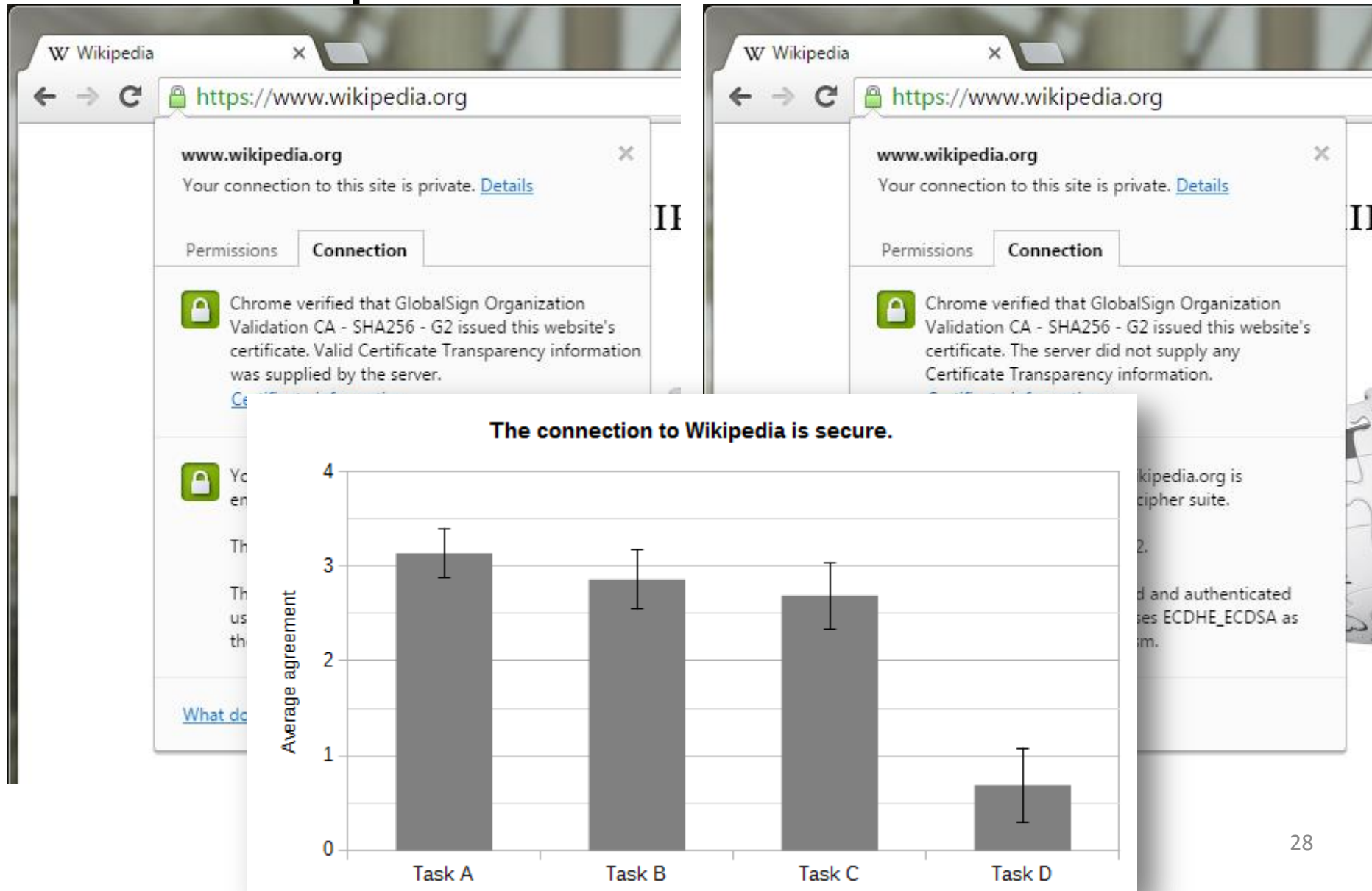
36 participants

- 33% female, 64% male, 3% preferred not to say
- 21 indicated occupation → 18 students

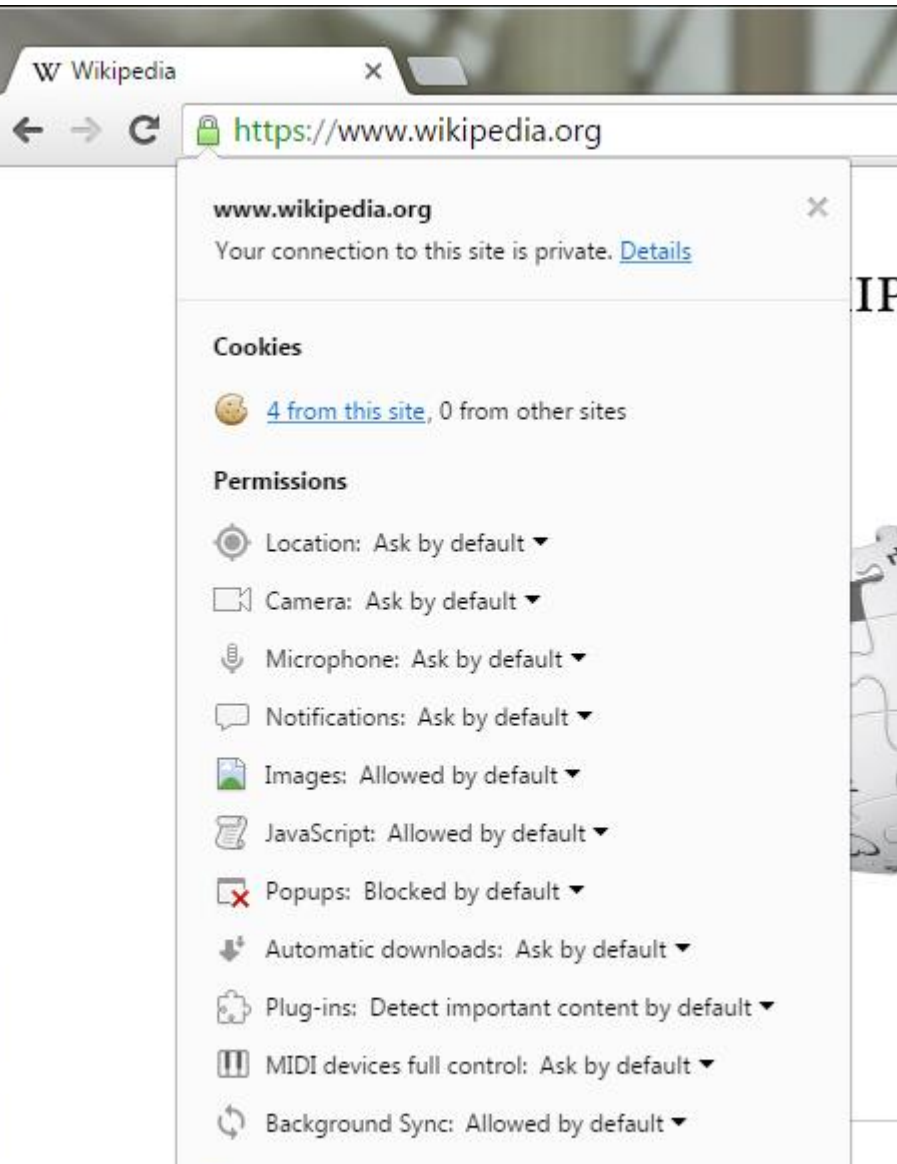


mean: 13.5
median: 12.5

Online questionnaire



Online questionnaire

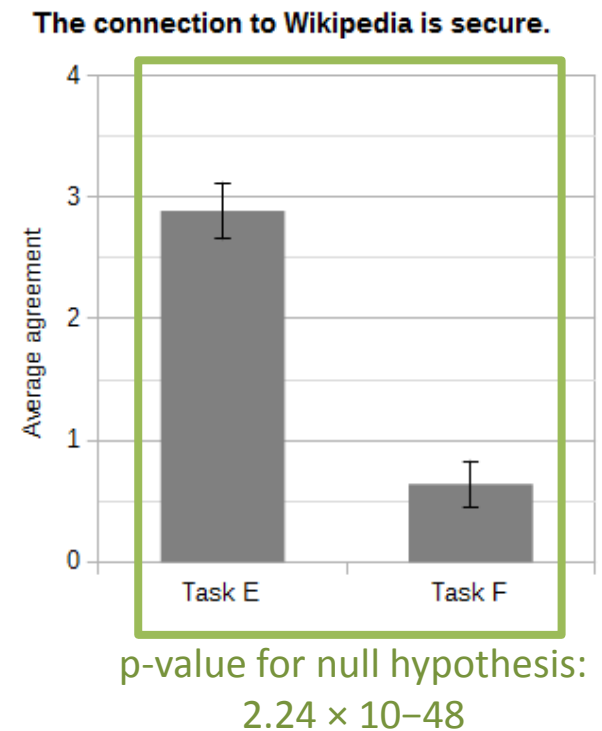
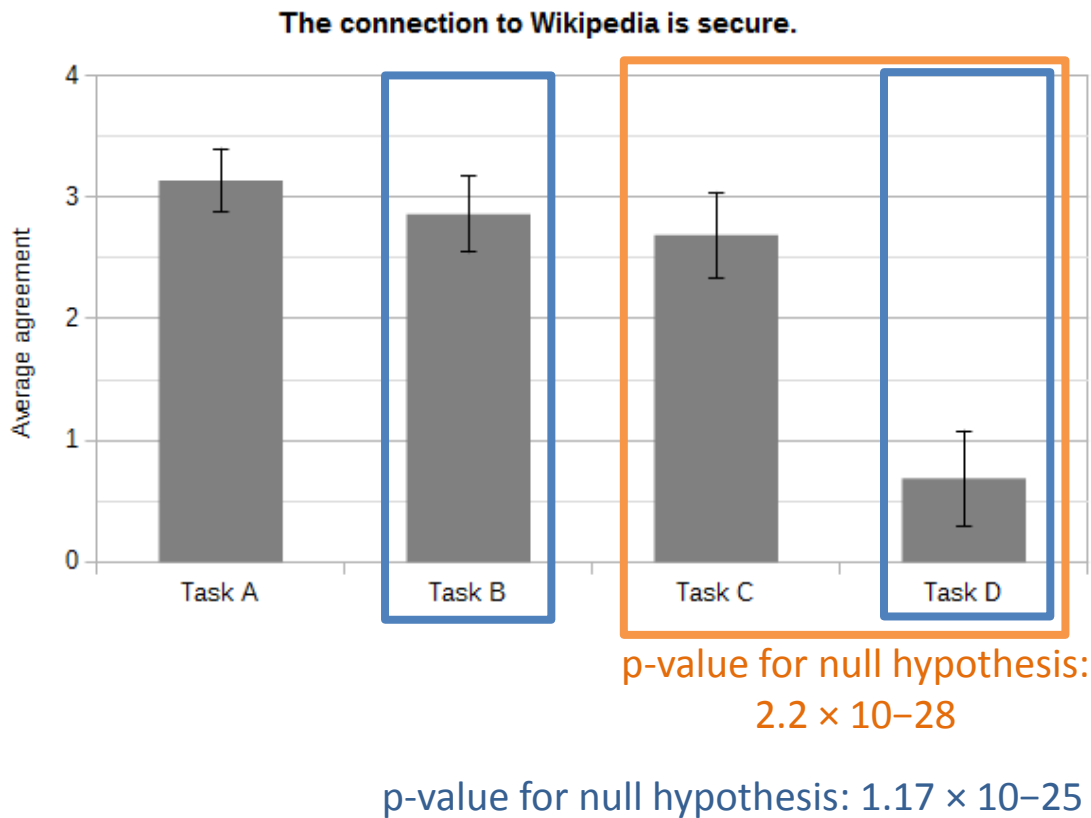


Confusing due to

- Information concerning the connection's security mixed up with cookies and permissions
- Too much information in general
- Too little information about security

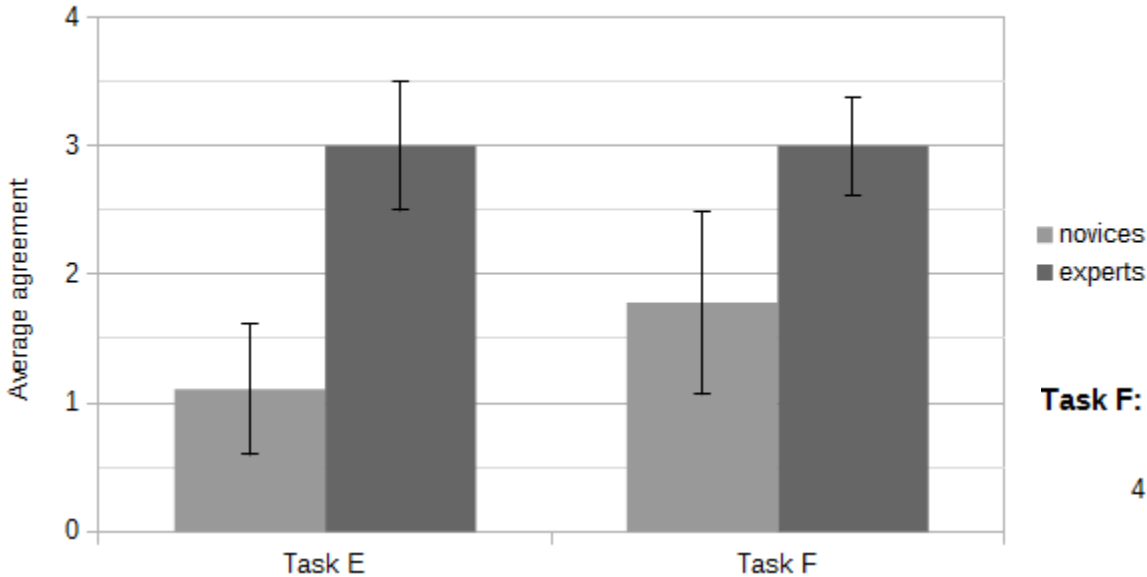
Online questionnaire

Error page shown in tasks D and F

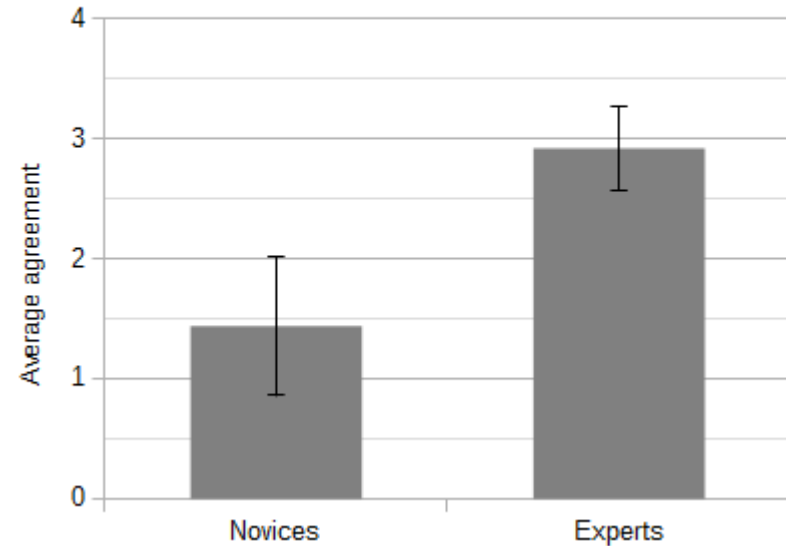


Online questionnaire

The information in the developer tools (DevTools) is helpful.



Task F: The information in the developer tools (DevTools) made it easy to understand the problem.



→ Mainly clarifications and explanations of terms

Limitations

- No representation of the whole user base of Google Chrome and Chromium
e.g. students
- Sampling bias due to self-selection of participants
e.g. topic, language



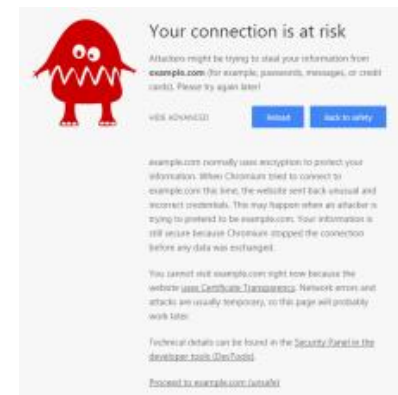
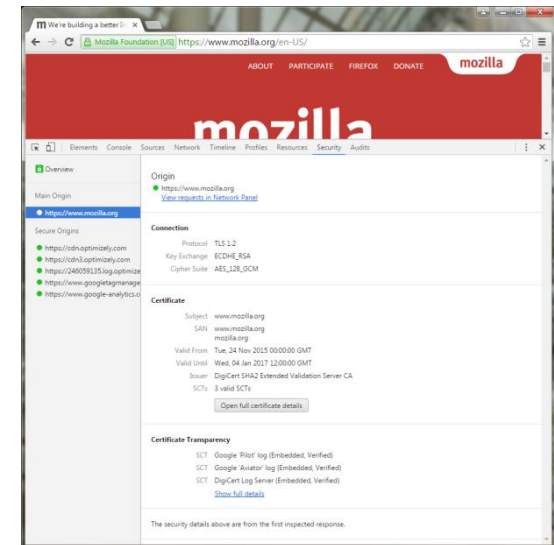
Future work



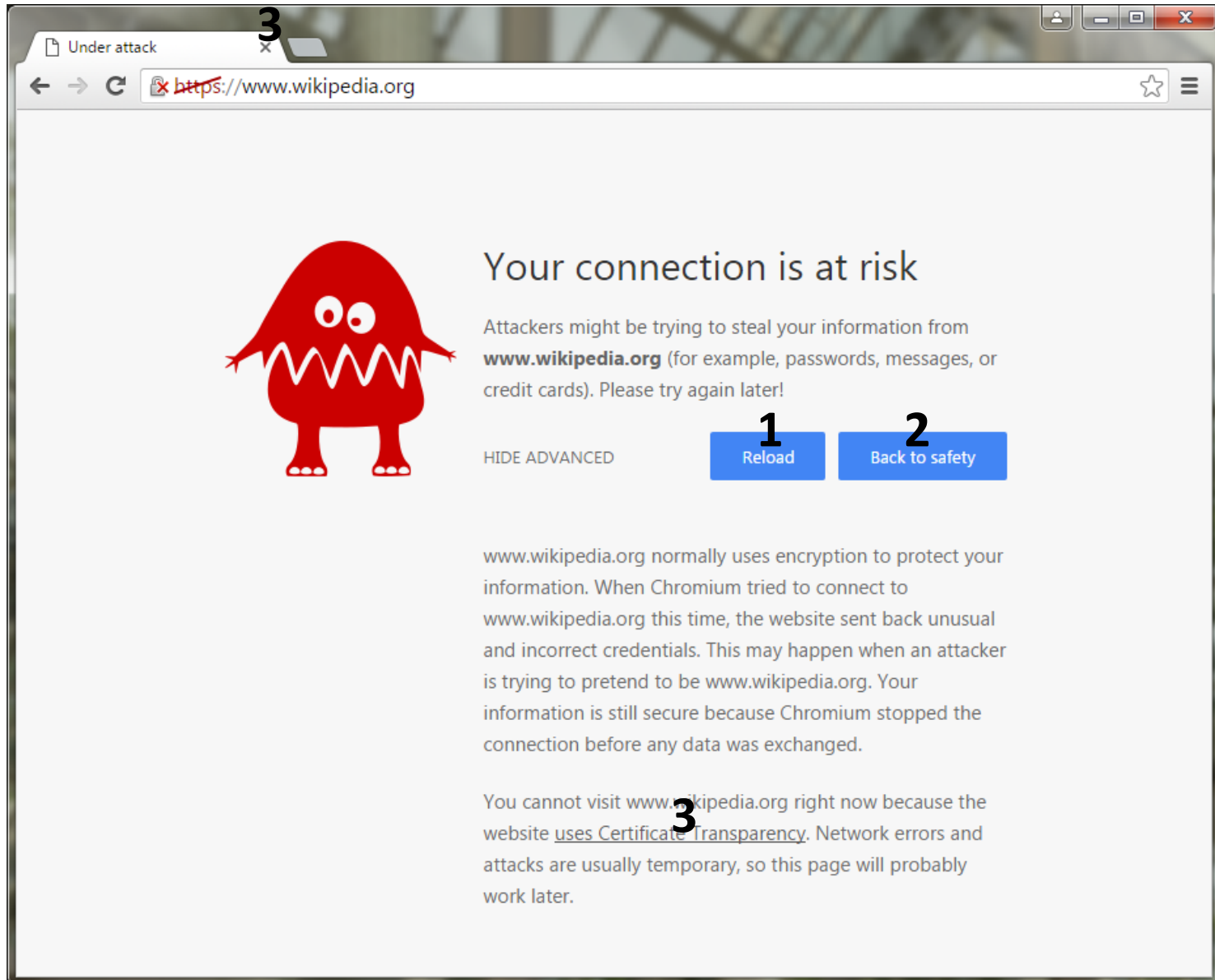
- Conservatively
 - More easy to reach and to understand explanations
 - Interactive tutorial in the DevTools
 - Notification when website is available over a secure connection again
 - Reminder after proceeding through error page
- Progressively
 - Rethink appearance of warnings → polymorphism
 - Standardisation of security indicators

Summary

- User-centred iterative design process
- Improved CT integration in Chromium by
 - Addition of CT details to DevTools
 - Suggestion of an error page for the case of a CT error
 - = 2826 lines of code, 931 contributed
- Suggested other improvements
 - Contacted by Google to continue



Online questionnaire




The screenshot shows a browser window with the address bar displaying <https://www.wikipedia.org>. The page title is "Under attack". The main content features a red cartoon monster icon on the left. To its right, the heading "Your connection is at risk" is displayed. Below this, a warning message states: "Attackers might be trying to steal your information from **www.wikipedia.org** (for example, passwords, messages, or credit cards). Please try again later!". Two blue buttons are present: "1 Reload" and "2 Back to safety". Below the buttons, a "HIDE ADVANCED" link is visible. A detailed explanation follows: "www.wikipedia.org normally uses encryption to protect your information. When Chromium tried to connect to www.wikipedia.org this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be www.wikipedia.org. Your information is still secure because Chromium stopped the connection before any data was exchanged." At the bottom, another paragraph states: "You cannot visit www.wikipedia.org right now because the website uses Certificate Transparency. Network errors and attacks are usually temporary, so this page will probably work later." The number "3" is overlaid on the browser window in three locations: the top-left corner, the address bar, and the text "www.wikipedia.org" in the bottom paragraph.

3

Under attack

3

← → ↻ ~~https://~~www.wikipedia.org ☆ ☰



Your connection is at risk

Attackers might be trying to steal your information from **www.wikipedia.org** (for example, passwords, messages, or credit cards). Please try again later!

HIDE ADVANCED

1 Reload 2 Back to safety

www.wikipedia.org normally uses encryption to protect your information. When Chromium tried to connect to www.wikipedia.org this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be www.wikipedia.org. Your information is still secure because Chromium stopped the connection before any data was exchanged.

You cannot visit www.wikipedia.org right now because the website uses Certificate Transparency. Network errors and attacks are usually temporary, so this page will probably work later.


3

Online questionnaire

3

Under attack x

← → ↻ ~~https://~~www.wikipedia.org ☆ ☰



Your connection is at risk

Attackers might be trying to steal your information from **www.wikipedia.org** (for example, passwords, messages, or credit cards). Please try again later!

HIDE ADVANCED

3 Reload 2 Back to safety

www.wikipedia.org normally uses encryption to protect your information. When Chromium tried to connect to www.wikipedia.org this time, the website sent back unusual and incorrect credentials. This may happen when an attacker is trying to pretend to be www.wikipedia.org. Your information is still secure because Chromium stopped the connection before any data was exchanged.

You cannot visit www.wikipedia.org right now because the website uses Certificate Transparency. Network errors and attacks are usually temporary, so this page will probably work later.

Technical details can be found in the Security Panel in the developer tools (DevTools).

1 [Proceed to www.wikipedia.org \(unsafe\)](https://www.wikipedia.org)

Digital attributions

- Anonymous hacker© Brian Klug CC BY-NC 2.0
- Business Meeting by parkjisun from the Noun Project
- Checklist by Aaron Dodson from the Noun Project
- clock by Dmitry Baranovskiy from the Noun Project
- Deploy by Razmig Getzoyan from the Noun Project
- Diploma by Andrew K Stauffer from the Noun Project
- electrocardiogram by Vectors Market from the Noun Project
- evaluate by Scott Lewis from the Noun Project
- Encryption by Gregor Črešnar from the Noun Project
- geek by Guilherme Simoes from the Noun Project
- grocery list by icon 54 from the Noun Project
- Laptop by Zoé Chartier from the Noun Project
- Light Bulb by Takao Umehara from the Noun Project
- Question designed by Anas Ramadan from The Noun Project
- Ribbon by Alex Auda Samora from the Noun Project
- Search by hunotika from the Noun Project
- Server by aLf from the Noun Project
- Sheep by Gira Park from the Noun Project
- Sleet and Ice © James Filipi CC BY-SA 2.0
- Smile by Vytautas Alech from the Noun Project