Securing the Open Web Platform

Web Security @W3C / MIT CSAIL
Wendy Seltzer, wseltzer@w3.org
@wseltzer
Insecurity
NTIA: Online Activities Avoided Due to Privacy or Security Concerns

% of Households with Internet Users, 2015

WWW, circa 1989

The WorldWideWeb (WWW) is a wide-area hypertext[1] information retrieval
initiative aiming to give universal access to a large universe of documents.

Everything there is online about WWW is linked directly or indirectly to this
document, including an executive summary[2] of the project, Mailing lists[3],
Policy[4], November's WWW news[5], Frequently Asked Questions[6].

What's out

there? [7]

What's out there? Pointers to the world’s online information,
subjects[8], WWW servers[9], etc.

Help[10]

on the browser you are using

Software

products[11]

Software Products: A list of WWW project components and their current
state. (e.g. Line Mode[12], X11 Viola[13], NetSTP[14], Servers[15], Tools[16], Mail
robot[17], Library[18])

Technical[19]

technical[19]

Technical Details: protocol, formats, program internals,
etc.

SIR TIM BERNERS-LEE
INVENTOR OF THE WORLD WIDE WEB
Director, W3C
The "http" scheme is used to locate network resources via the HTTP protocol. [RFC 2616, 1999]

http_URL = "http: //" host [ ":" port ] [ abs_path [ "?" query ]]

<HTML>
  <HEAD>
    <TITLE>Hello World</TITLE>
  </HEAD>
  <BODY><P><A HREF="https://anywhere.example/">I can link anywhere!</A></P>
  </BODY>
</HTML>

(still valid in HTML5, 2014)
The Generative Web
A Proprietary Platform

Apple sells:

Hardware

Operating system

Software - only approved apps
Who owns security on an open platform?
From Tragedy to Comedy of the Commons
World Wide Web Consortium (W3C)

Voluntary standard-setting. Stewards of the Open Web Platform.

Addressing the collective action challenge of Web security

Modular security

- Component by component (end-to-end)
- Foundations for trust and secure communication

Incentive: keep the platform working jointly, compete on top
Assessing “Security”

Confidentiality, Availability, Integrity?

Rapid deployment, ease of interop, extensibility

Correct operation?

The Web has 404s
but browsers try very hard to render whatever they’re presented

Postel’s Law (robustness)?

“Be conservative in what you do, be liberal in what you accept from others.” [RFC 761, 1980]
Security

For what? from what?

Threat models vary with users and uses of the Web.
Security

For what? from what?

Threat models vary with users and uses of the Web.

One person’s “insecurity” may be another’s “feature”
Is this a (fl|ph)ish?

Why yes, I am a fish. rling.com
Is this?
Make Sign-on Credentials Unphishable

WebAuthn, building a Web API for FIDO 2.0, uses a cryptographic challenge **unique** to each website and **bound** to its origin.

Local authentication such as biometrics never leaves the device.
Mint. It’s all coming together.

Mint makes managing your personal finances a cinch. Be the master of your money so you can get more out of life.

SIGN UP FREE

The complete picture in minutes

See all your balances and transactions together. Mint automatically pulls all your financial information into one place, so you can finally get the entire picture.
CORS

Cross-Origin Resource Sharing, aka opening closed systems to interop, with care
W3C WebAppSec

Enlisting the User Agent in Cooperative Policy Enforcement

- Content Security Policy
- Subresource Integrity
- Mixed Content Blocking

Security Related APIs

- Permissions API
- Credential Management

Experiments in the Web Security Model / Same Origin Policy

- Confinement with Origin Web Labels (COWL)
Interception or Assistance?

- Spam filtering
- Video and image compression
- Traffic management
- Quality of service
W3C TAG Findings

- Securing the Web. W3C TAG Finding, January 2015
  - https://www.w3.org/2001/tag/doc/web-https

  - https://www.w3.org/2001/tag/doc/encryption-finding/
Encryption Everywhere

WebAppSec Standardizing and Enabling HTTPS for confidentiality, integrity, and authentication

- Secure Contexts
- Upgrade Insecure Requests
- Mixed Content
- Referrer Policy
- Subresource Integrity

- Let's Encrypt
- Certificate Transparency
- HSTS, HPKP

IETF
WebCrypto API

Enable web application developers to build on standard javascript crypto across browsers.

OpenWhisper’s Signal desktop

PKI.js

PKI.js is a pure JavaScript library implementing the formats that are used in PKI applications (signing, encryption, certificate requests, OCSP and TSP requests/responses). It is built on WebCrypto (Web Cryptography API) and requires no plug-ins.
Emergent Security Model of the Web

Strong authentication protects users and applications

Browser cooperates with the WebApp developer (origin) in security-policy enforcement, on behalf of the user.

Same-origin policy scopes data interchange.

Encryption (TLS, HTTPS) provides confidential, authenticated, integrity-protected channel.
Opening Closed Systems Is Hard to Do Right

Open CAN bus + unprotected inputs

- ODB-II
- MP3 CD
- Bluetooth
- OnStar
- ...
ZVT and Poseidon are not secure by design

<table>
<thead>
<tr>
<th>Vulnerability root causes</th>
<th>Poseidon</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZVT</td>
<td>Poseidon</td>
</tr>
<tr>
<td>System-wide signature keys</td>
<td>System-wide auth keys</td>
</tr>
<tr>
<td>Used with symmetric crypto</td>
<td>Also, but not making matters worse:</td>
</tr>
<tr>
<td>Stored in insecure HSMs</td>
<td>Stored in insecure HSMs</td>
</tr>
</tbody>
</table>

Both protocols mix “security through obscurity” (system-wide keys) with “security certification” (HSMs). Neither implements “security by design”
Security and Privacy Considerations Everywhere

Build for Open.

Review, review, review!

Make spec authors think about -- and mitigate -- security and privacy risks.

Offer guidance to developers using these specs.
The Web’s Multi-Use Commons
On an open platform

We can’t predict user intent

We don’t control the ecosystem

Incentives vary

Users!
User sovereignty / Security as delegation

In the priority of constituencies, users come first.

“In case of conflict, consider users over authors over implementors over specifiers over theoretical purity. In other words costs or difficulties to the user should be given more weight than costs to authors....”

Does that mean we should just do whatever the user asks?

Users are rarely security experts, often (rationally) choose convenience.

Security through delegation; the browser is “user-agent.”

Encryption (with effective key management) makes participation explicit.
Meeting User Expectations

Giving users the tools by which to set and assess expectations

+ feedback by which they can update understanding
Instead of “trust the platform,” build a toolbox for trust among users

End-to-End = local self-determination

Modularize

Encrypt everywhere

Build for Open

Enlist and enable the user
Links

Overview of Security at W3C: [https://www.w3.org/Security](https://www.w3.org/Security)

WebCrypto: [https://www.w3.org/TR/WebCryptoAPI/](https://www.w3.org/TR/WebCryptoAPI/)

WebAppSec: [https://www.w3.org/2011/webappsec/](https://www.w3.org/2011/webappsec/)

Web Authentication: [https://w3c.github.io/webauthn/](https://w3c.github.io/webauthn/)

Hardware-Based Secure Services: [https://www.w3.org/community/hb-secure-services/](https://www.w3.org/community/hb-secure-services/)
Thanks!

Wendy Seltzer
wseltzer@w3.org https://wendy.seltzer.org/
@wseltzer +1.617.715.4883
Image credits


Authentication Diagram, FIDO Alliance, https://fidoalliance.org/specifications/additional-resources/

Cattle, Peter O'Connor aka anemoneprojectors, Henley-on-Thames 049: Greys Court

Masks, Booyabazooka, Drama-icon.svg, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1588838

Core, giddygoose, https://www.flickr.com/photos/giddygoose/3312544386

Man in the Middle, Jorge Reyes, The Noun Project, thenounproject.com

Shopshifting, 32C3, https://media.ccc.de/v/32c3-7368-shopshifting

Multitool, leatherman.com