

Is Your Browser a User Agent or a Double Agent?

SESSION ID: **DSP-R04A**

Mike Shema

Director of Engineering
Qualys, Inc.

@CodexWebSecurum

Agents — User, Double, and Secret

We use browsers to access sites. *(Sites use our data.)*

Browsers are inching towards “default secure”.

We haven’t reached “default private”. *(If we even can.)*

There’s a lot to fix.

Browser Security (My system)

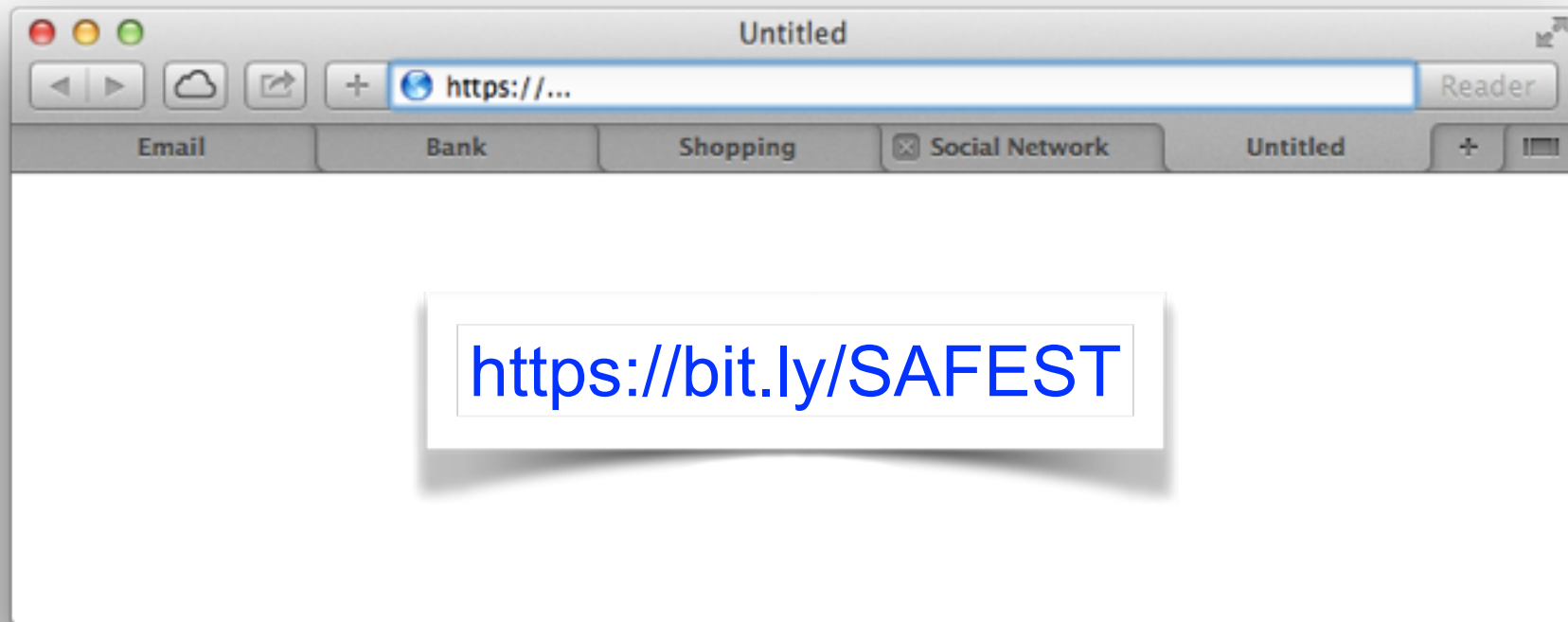
Self-update eases patch maintenance.

Process separation inhibits exploits.

SSL settings prioritize recommended protocols.

(Myself) Data Security

The Harry Callahan Postulate



Secure Browser, Insecure Web App

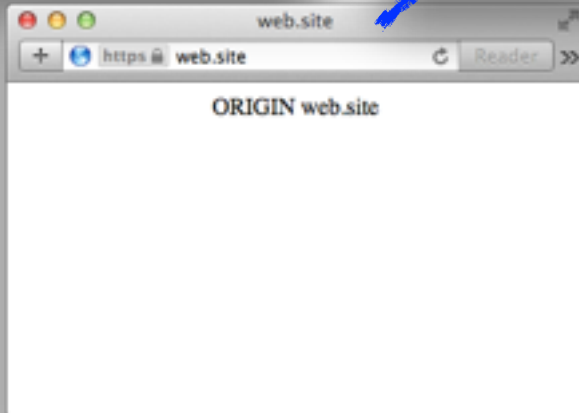
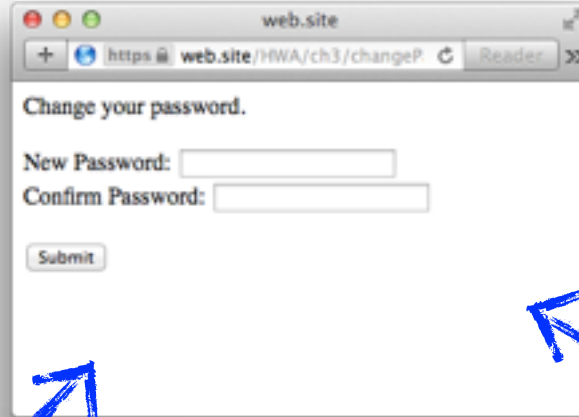
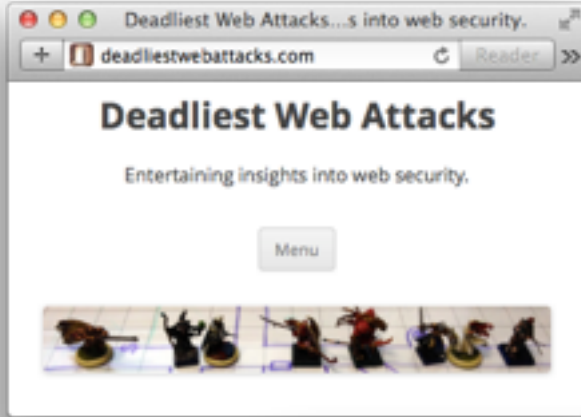
Lack of transport security — Sniffing

Unrestricted resource framing — Clickjacking

Inadequate state enforcement — CSRF

Beacons, Cookies, Likes — Privacy

Same Origin Is Only Some Isolation



```
<form action="https://web.site/...">
<input type="hidden" name="pass">
<input type="hidden" name="pass_confirm">
<input type="submit">
</form>

<script src="https://web.site/..."></script>
```

Advertising Is Inherently Cross Origin

User data consumption

Malware delivery system

Intrusive content



http://bit.ly/java_ad

Resource Isolation vs. Site Isolation

HTTP Strict Transport Security

Content Security Policy

Cross Origin Resource Sharing

<iframe> sandbox

Mobile Reinvents Security Failures

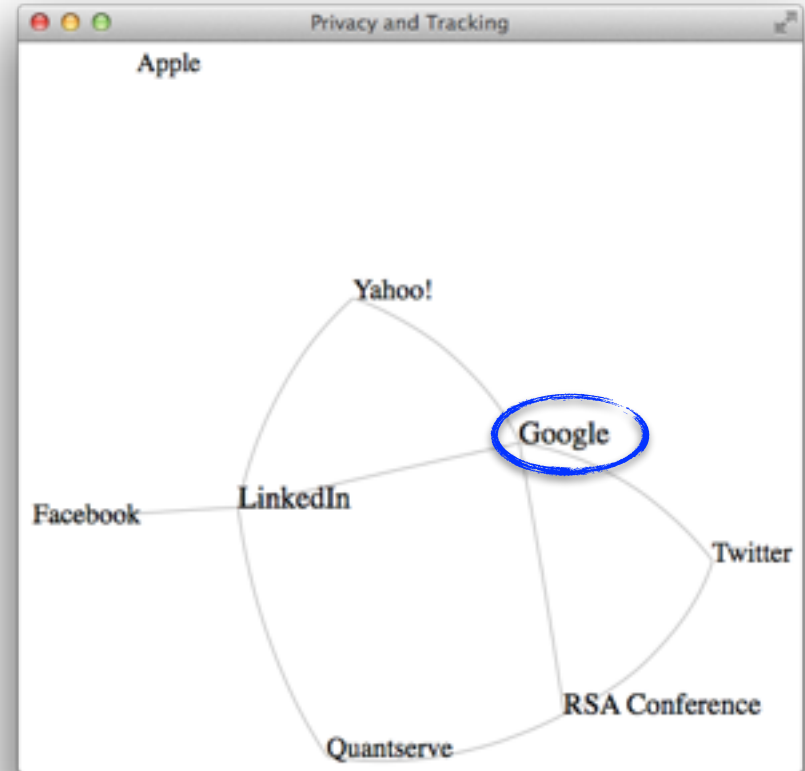
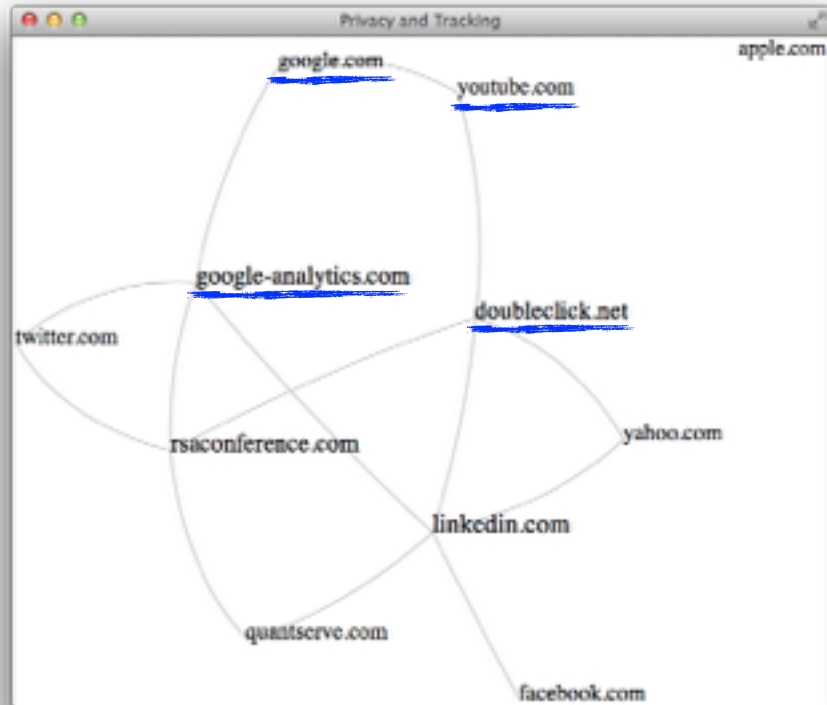
Misuse HTTPS

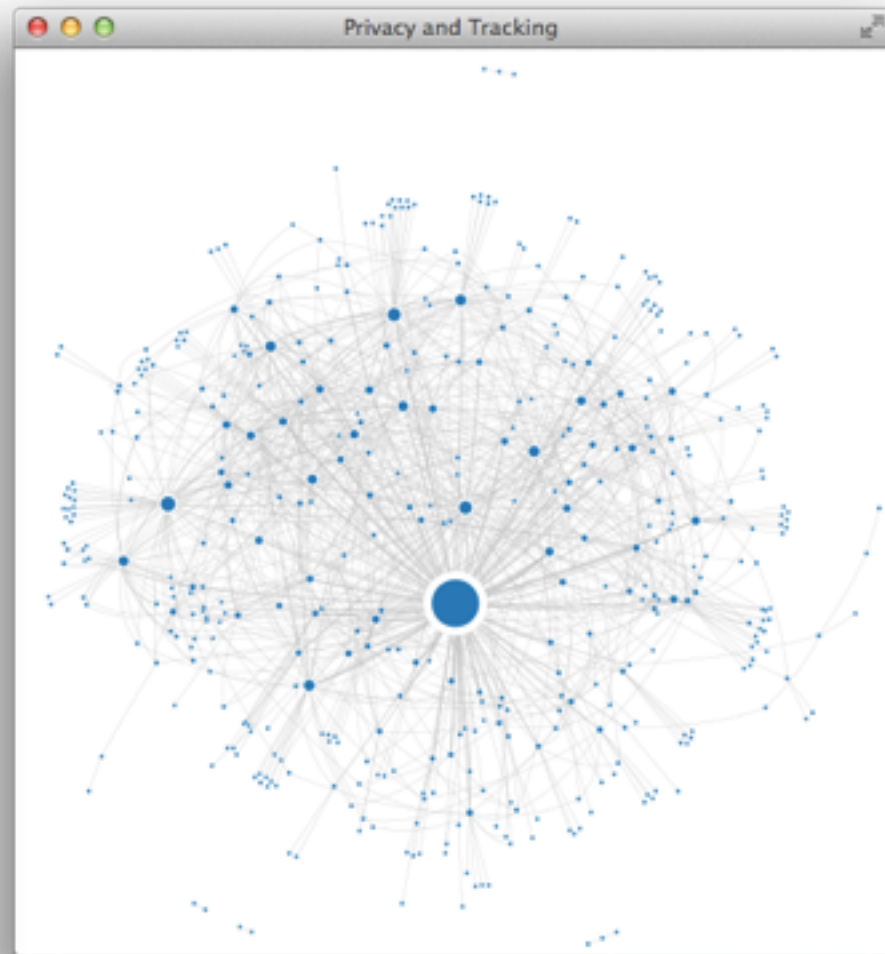
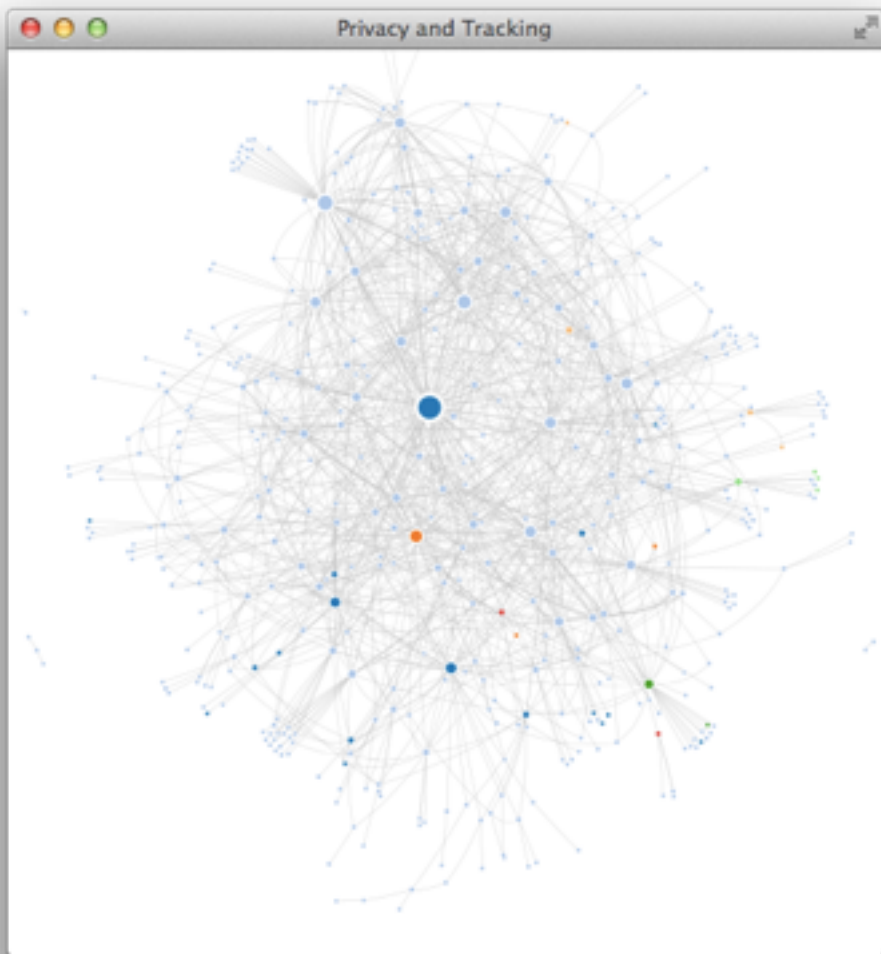
Omit certificate validation
(browsers have adopted certificate pinning)

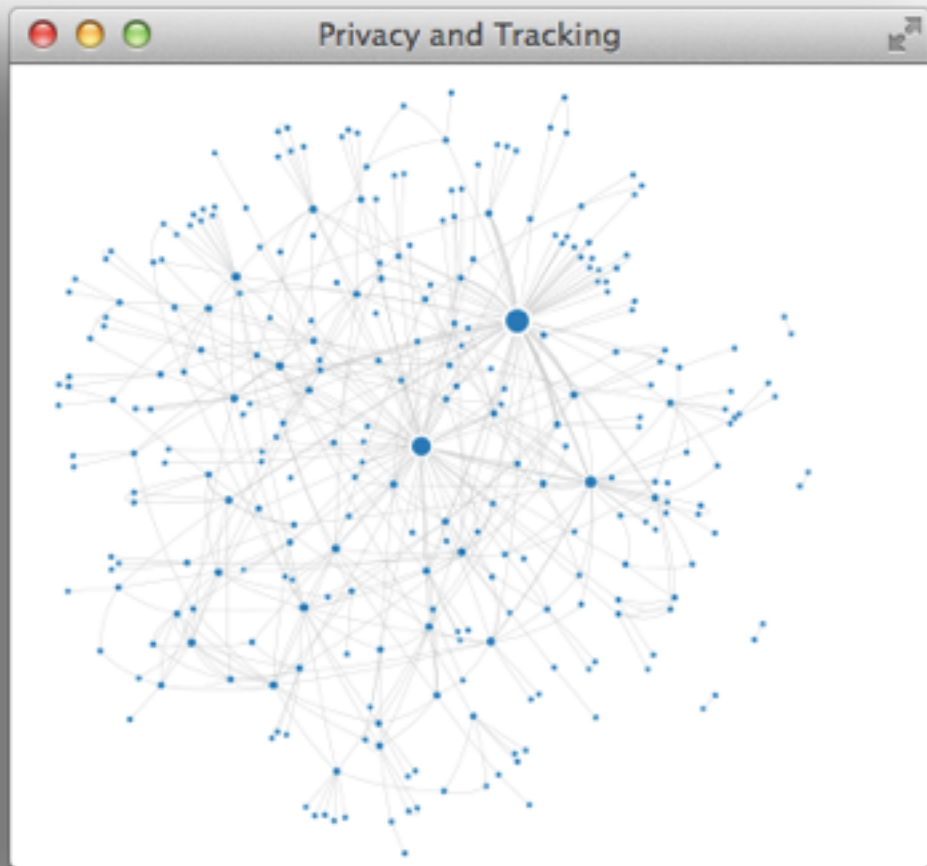
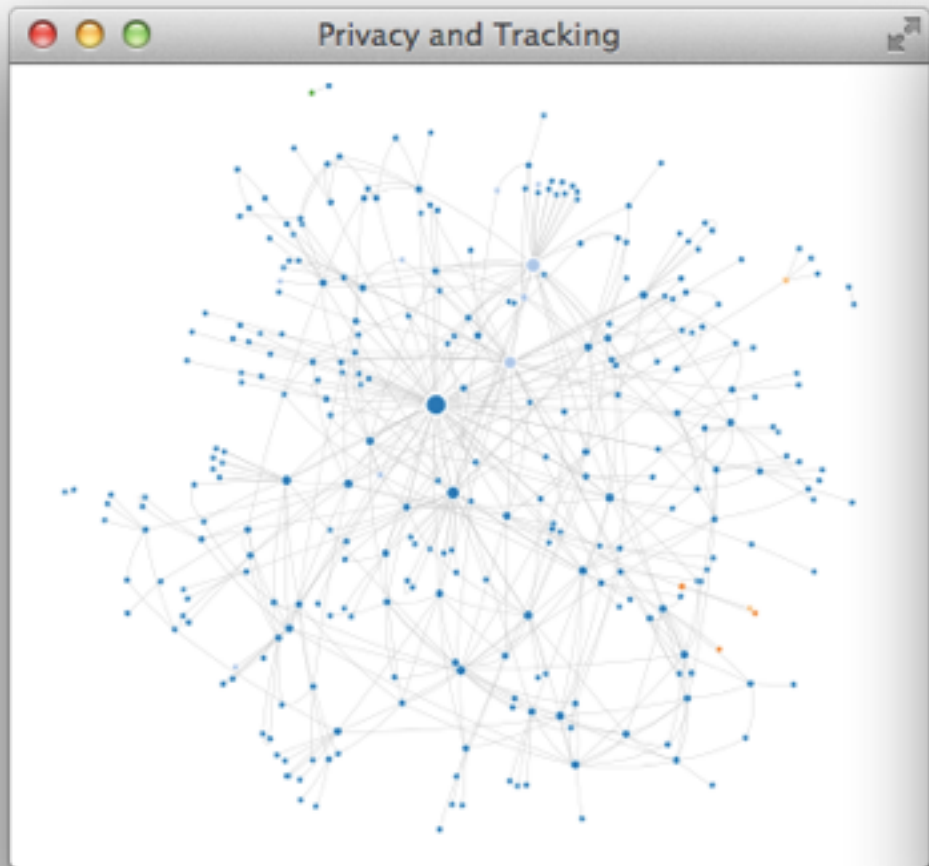
Plaintext storage on device

Data grabs

Resource Isolation, Data De-Isolation







Data Isolation and Constellations

Passwords

Personal info

Sensitive info

The threats of aggregation

[More Graph Demos]

Mobile and Browser Privacy

Personas

Protection

Penalties

Persistence

Pollution

Implementation Spectrums

Client ————— Server

User ————— Provider

Technical ————— Policy

Bring the User Agent Back to Users

Default deny third-party cookies

Same Origin Policy isn't a privacy barrier

Identity management

“Context Vaults” — Tab-specific isolation

Cookie Jar, Web Storage API, plugins, ...

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Thank You!

References

<http://d3js.org>

<http://www.mozilla.org/en-US/lightbeam/>

<https://github.com/mozilla/lightbeam>

Latest slides at <http://deadliestwebattacks.com>