RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Building and Breaking Privacy Barriers

SESSION ID: **CDS-W07**

Mike Shema

Director of Engineering
Qualys, Inc.
@CodexWebSecurum

QUALYS

# Agents: User, Double, Secret

Browsers are placing more components and content in sandboxes. This **resource isolation** creates a more secure environment by default.

But privacy also requires **data isolation**.

# The Great Barrier Grief

The Browser — A delicate ecosystem for rendering an abundance of sites, under pressure from aggregating innumerable origins, threatened by hazardous content and encroaching datavores.

# Browser Security (My system)

Automatic self-update assures prompt patching.

Process separation inhibits exploits.

SSL/TLS prioritizes recommended protocols and ciphers.

## (Myself) Data Security

# Some In-Browser Barriers

## Security

Same Origin Policy

Cookie Policies

HTML5 Sandboxes

Content Security Policy

~~Plugins~~

## Privacy

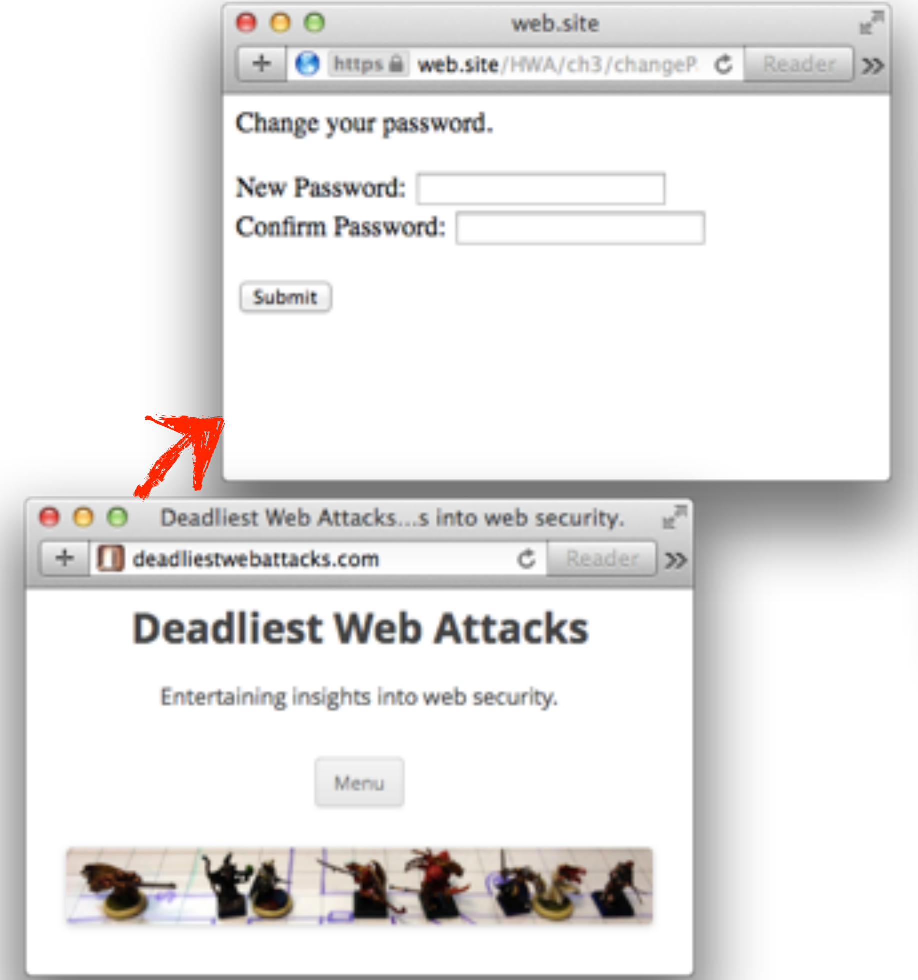
P3P ☹

Cookie Policies

Do Not Track ☹

# Same Origin Is Only Some Isolation

## CSRF [Forge]



web.site

https web.site/HWA/ch3/changeP

Change your password.

New Password:

Confirm Password:

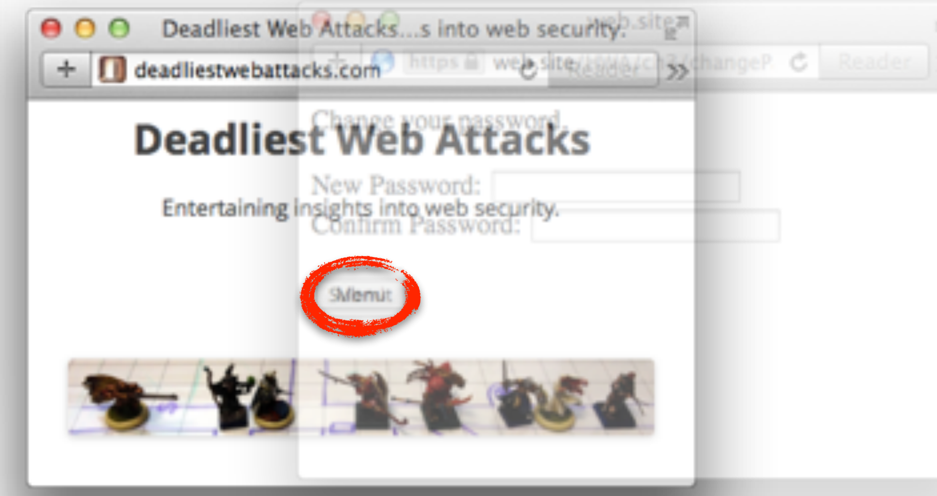
Deadliest Web Attacks...s into web security.

deadliestwebattacks.com

Deadliest Web Attacks

Entertaining insights into web security.

## Clickjacking [Overlay]



Deadliest Web Attacks...s into web security.

deadliestwebattacks.com

Deadliest Web Attacks

Entertaining insights into web security.

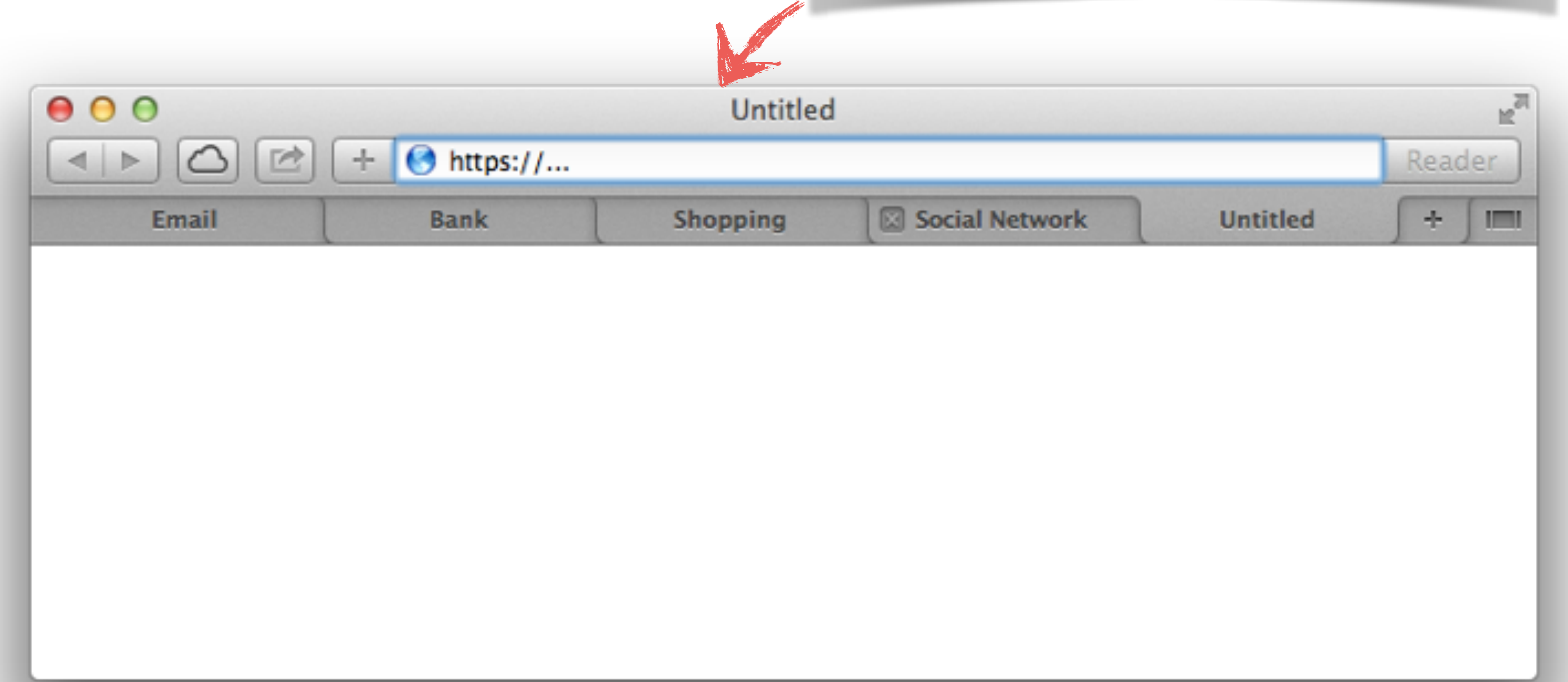
Change your password.

New Password:

Confirm Password:

# Keeping Tabs On Your Data

https://bit.ly/SAFEST



# The Parallax of Privacy

These examples focus on **technical controls**, e.g. a trusted client running untrusted code.

Effective enforcement may also require policy, legal, or social controls.

# Desirable Attributes

Durational Relevance — Works against immediate and long-term attacks.

Internal Isolation — Minimal data exposure to authorized users, i.e. least privilege access.

Disassociation (External Isolation) — Minimal correlative potential with other data sets.

# Security Failures Impact Privacy

**Absence** of transport security exposes data to sniffing and intermediation.

**Inadequacy** of state enforcement enables browser activity within a user's context.

**Confusion** of interface layering misleads user activity within a security context.

# Feature Abuse Impacts Privacy

System

Java LiveConnect

```
new Socket(host, port).getLocalAddress().getHostAddress();
```

WebRTC

```
var RTCPeerConnection = window.webkitRTCPeerConnection ||
window.mozRTCPeerConnection;
```

```
* beef/modules/host/get_internal_ip
  beef/modules/host/get_internal_ip_webrtc
```

Browser

Screenshots with <canvas> (limited)

```
* http://html2canvas.hertzen.com
```

Fingerprinting with <canvas>

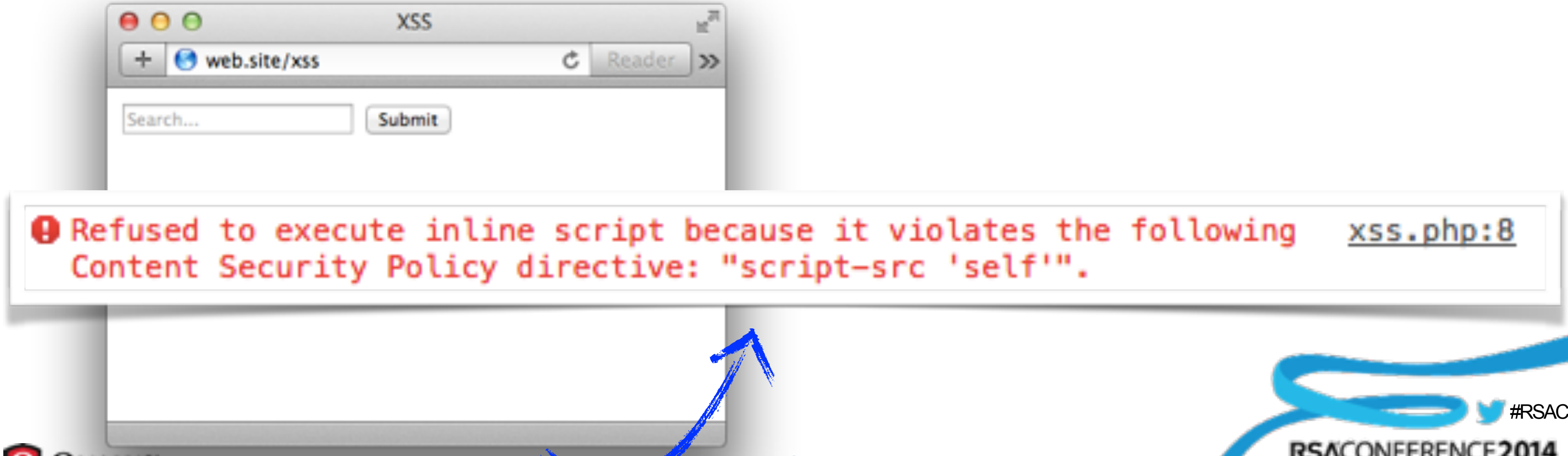
User

Mouse tracking exfiltration via WebSockets

# [Example] CSP

Positive security model to control resource origins and JavaScript execution.

```
Content-Security-Policy: script-src 'self'
...
<input type="text" name="q" value=""~~"><script>alert(9)</script>~~">
...
```

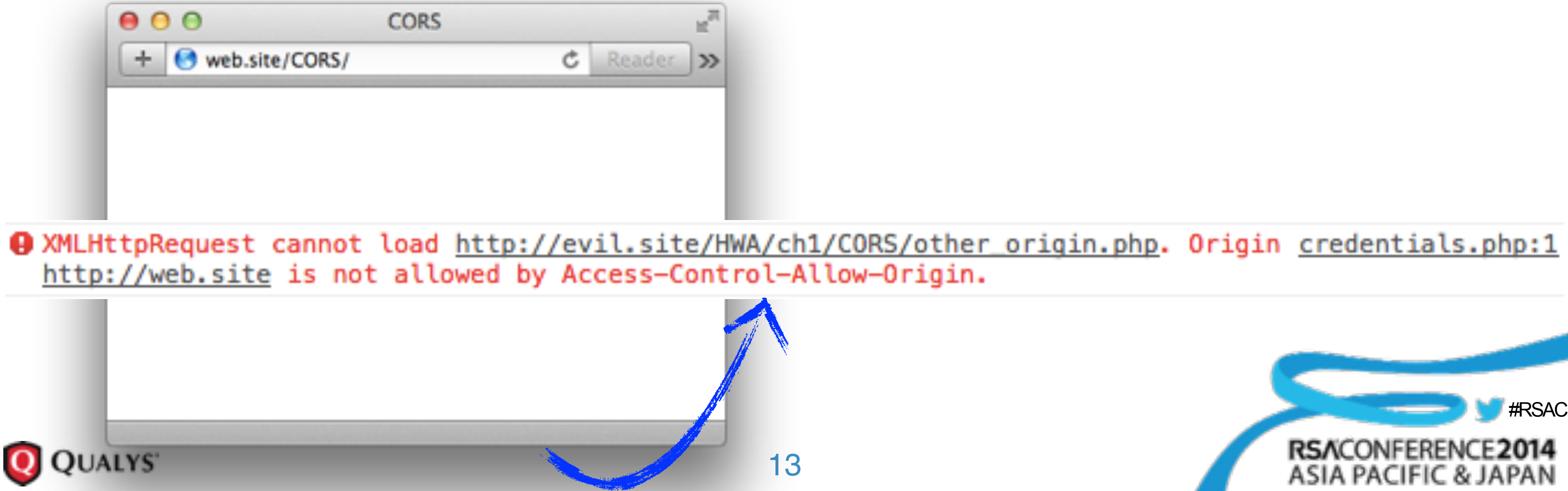


```
Refused to execute inline script because it violates the following    xss.php:8
Content Security Policy directive: "script-src 'self'".
```

# [Example] CORS

Positive security model to control read access to resources in mixed-origin content.

```
Access-Control-Allow-Origin: http://web.site
Access-Control-Allow-Methods: GET
Access-Control-Max-Age: 10
```

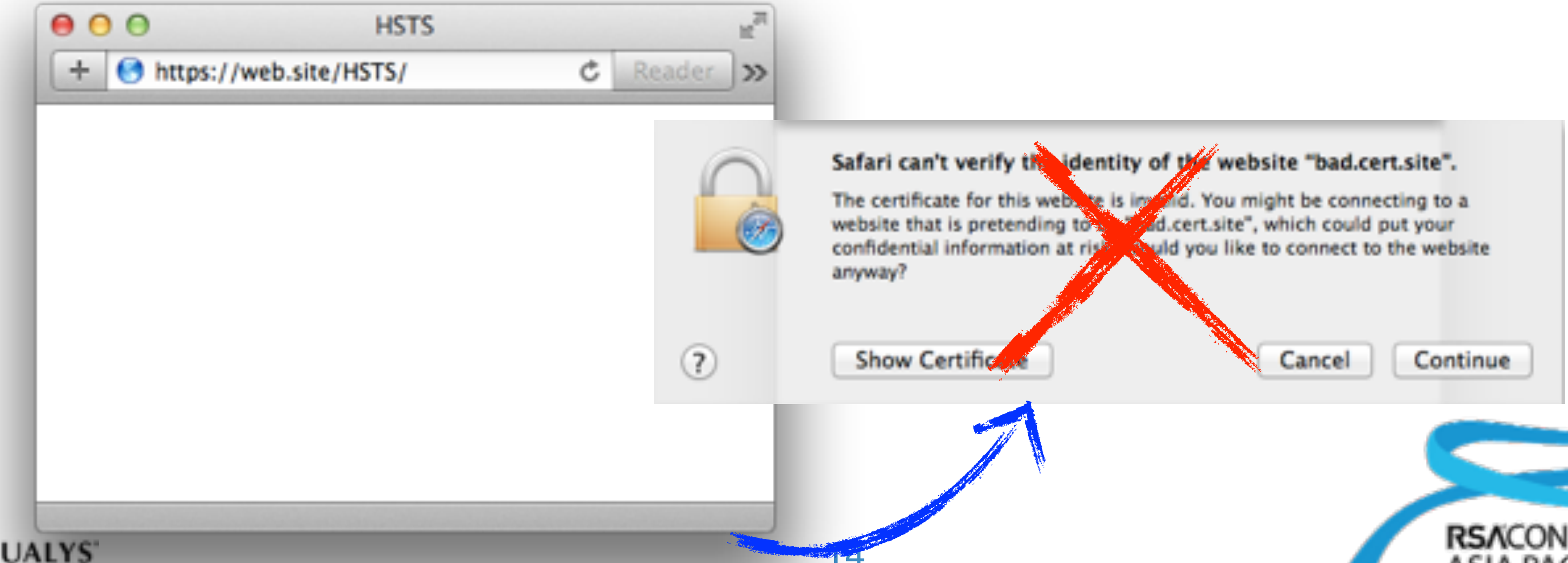


```
XMLHttpRequest cannot load http://evil.site/HWA/ch1/CORS/other_origin.php. Origin credentials.php:1
http://web.site is not allowed by Access-Control-Allow-Origin.
```

# [Example] HSTS

Instruct the client to force https schemes for the origin and terminate https connections that are in error or produce warnings.

```
Strict-Transport-Security: max-age=2592000
```



Safari can't verify the identity of the website "bad.cert.site".

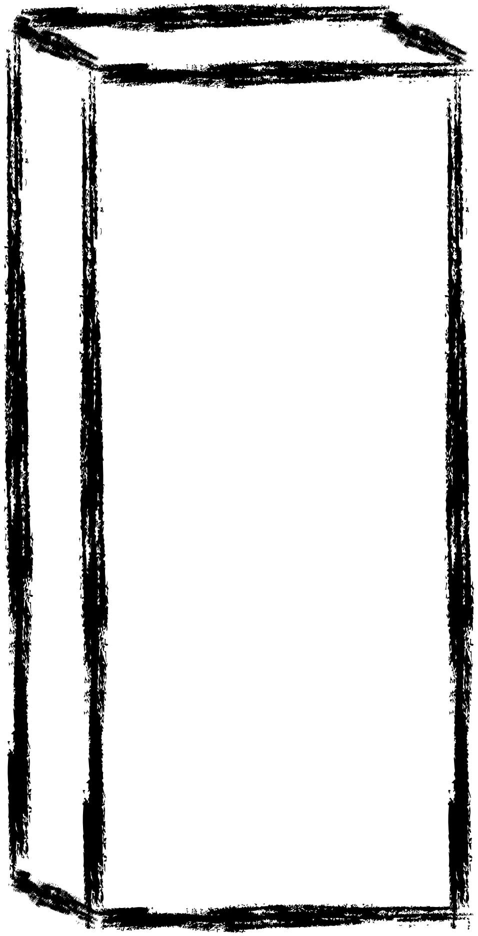
The certificate for this website is invalid. You might be connecting to a website that is pretending to be "bad.cert.site", which could put your confidential information at risk. Would you like to connect to the website anyway?

# Site, Origin, Resource, …

We've isolated resources and execution with CSP, used CORS to broaden resource access for explicit origins and duration, and used HSTS to isolate origins with encrypted traffic.

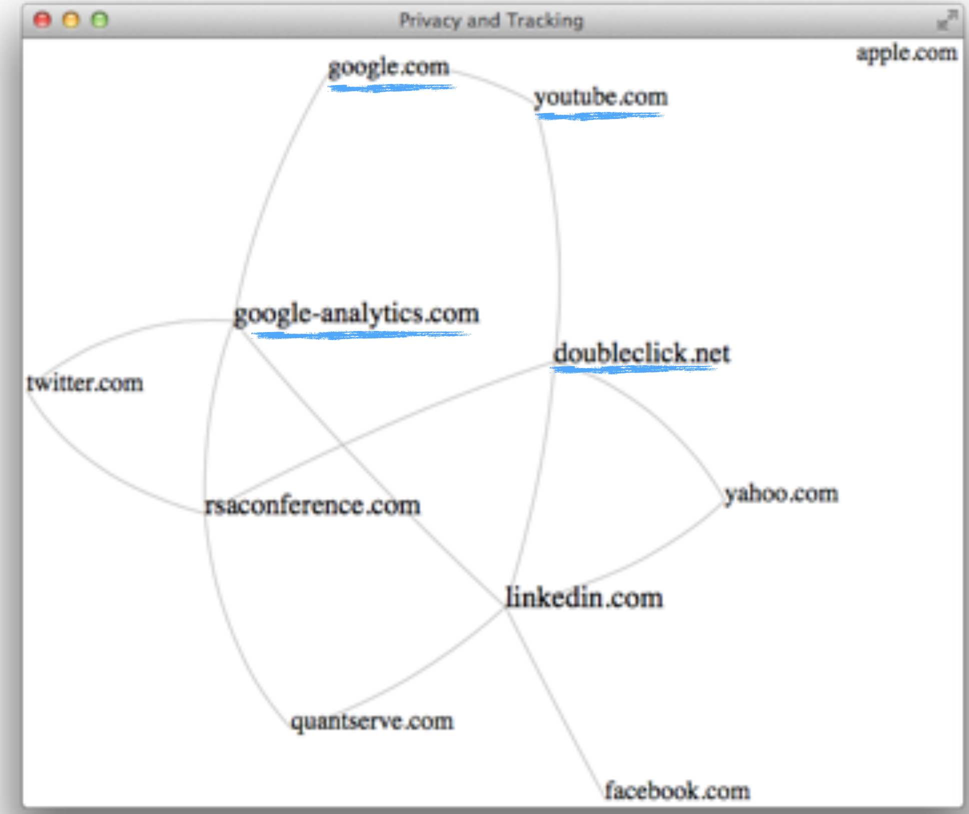
But have we improved data isolation?

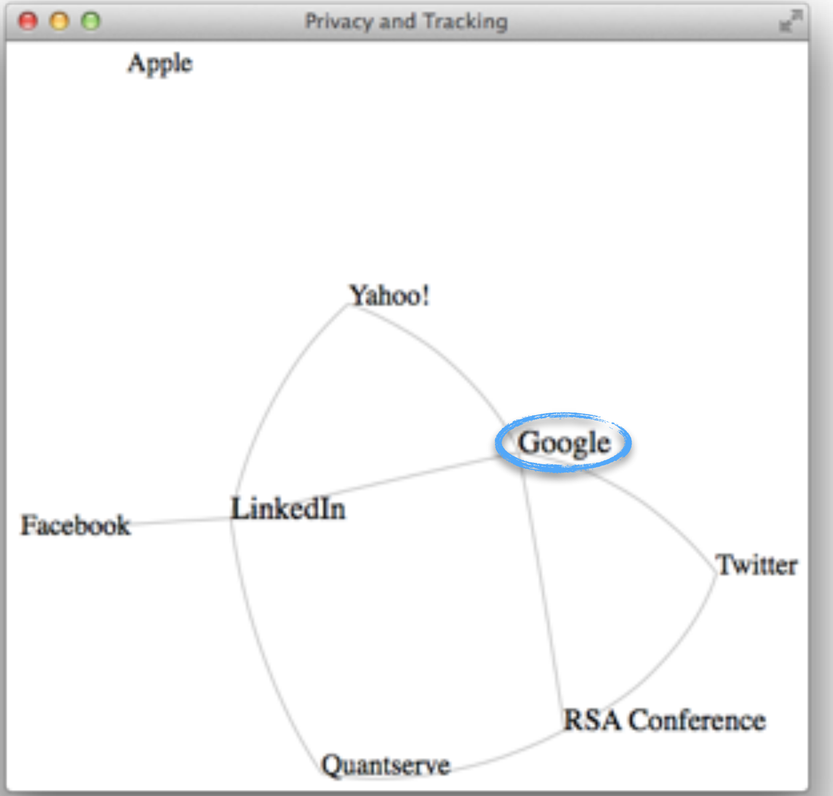
# Constellations of Isolation



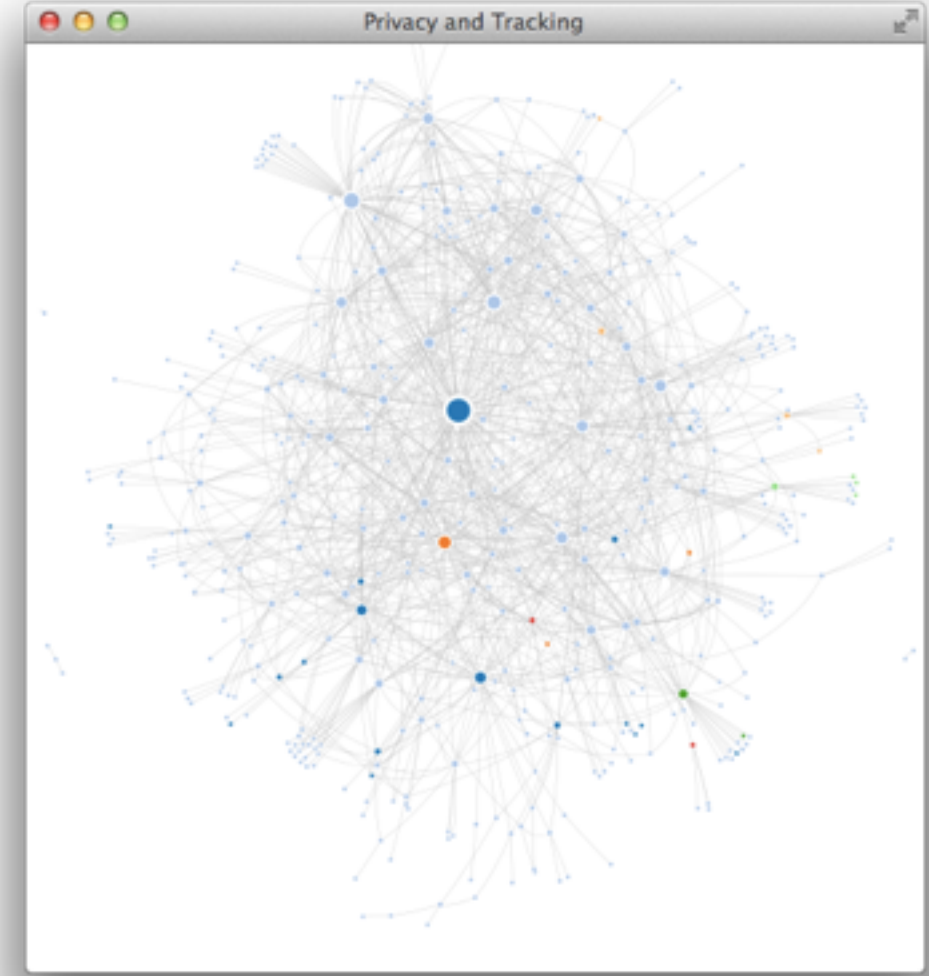
*"—it's full of stars!"*

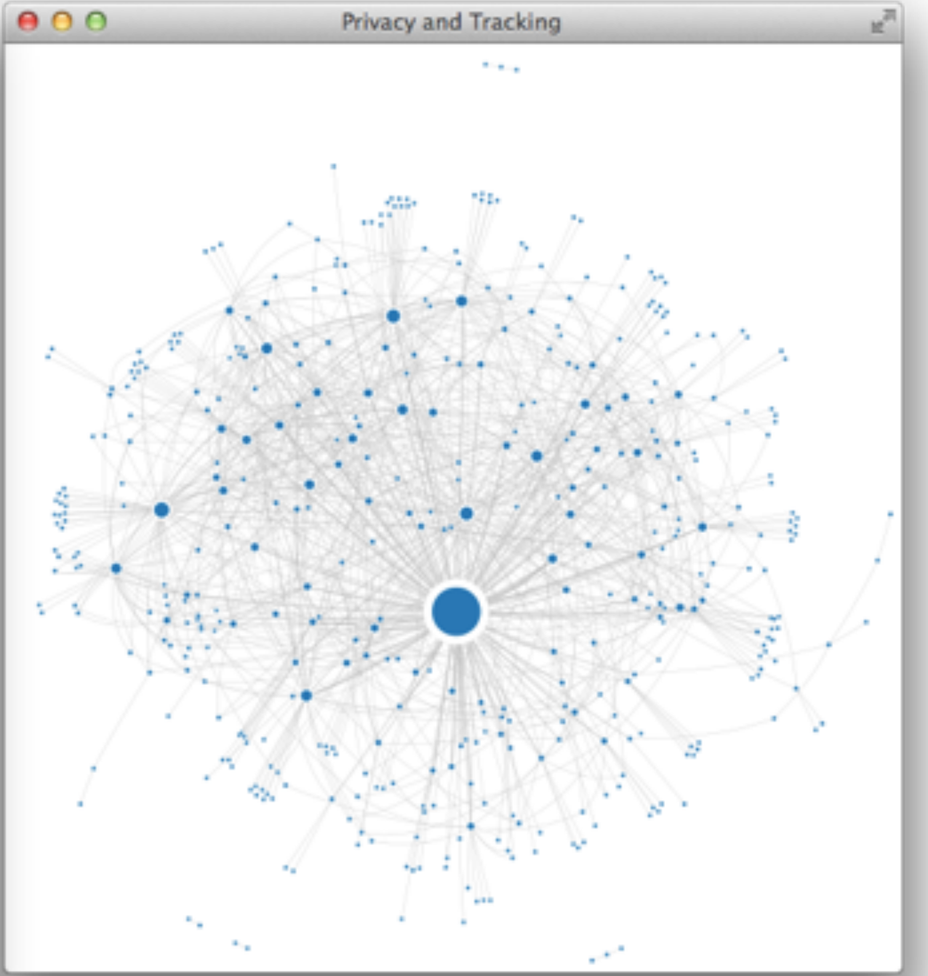
# Resource Isolation, Data De-Isolation



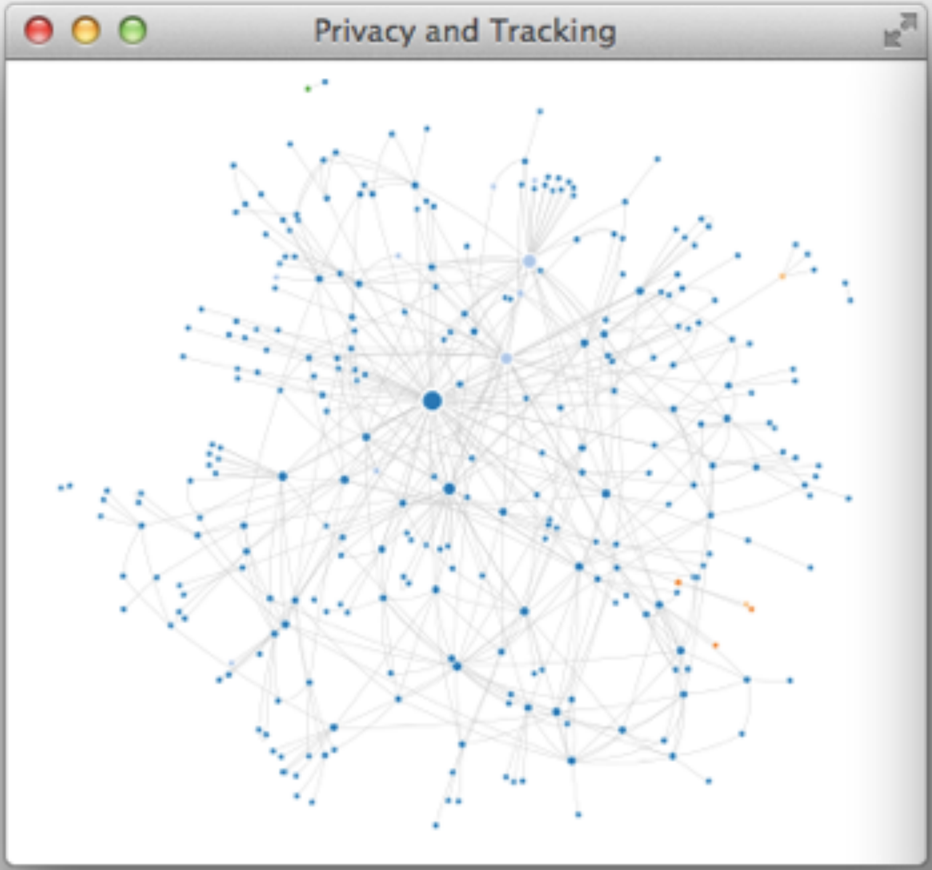


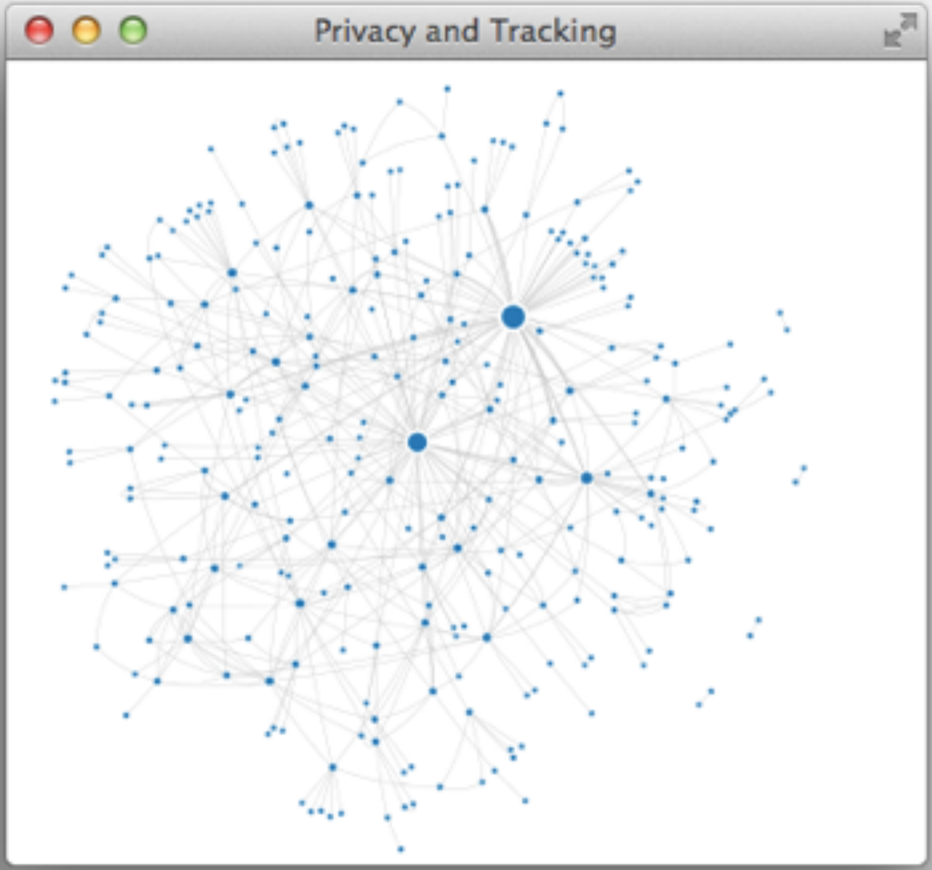
# Resource Isolation, Data De-Isolation

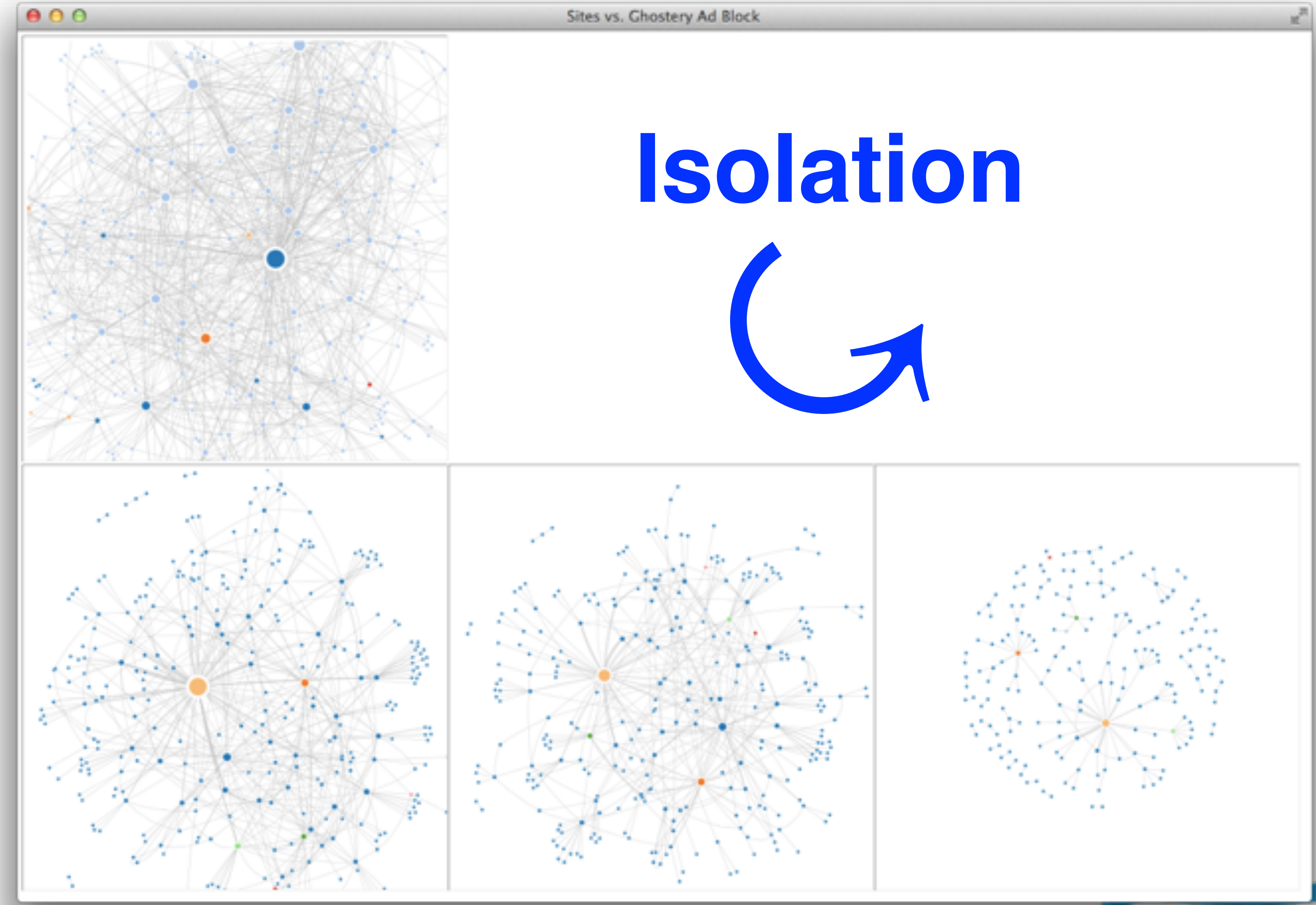




# Resource Isolation, Data De-Isolation







Isolation

# Stellar Collapse

One mistake where a tracking cookie ties two isolated profiles back together.

Correlation with other data sets may de-anonymize profiles.

> *In a world with one eye on privacy, the blind browser is king.*

# [Review] Same Origin Policy

Restricts read access to a resource, doesn’t restrict “simple” requests for a resource (e.g. web beacons, CSRF).

Mixed origin content can be secure and still be a threat to privacy.

# Consider Cookie Policies

Ambiguous relationships between first- and third-party status. [Inadequacy]

First-party status implies recency, not permanency. [Durational Relevance]

Merely one manner of tracking.

# Learning from Weaknesses

Timing inference that reveals data based on caches, algorithms, etc.

Data leaks due to incomplete controls.

Side-channel attacks against missing controls.

# Passwords as Private Data

Sharing a secret between two parties.

```
singapore
```

Means they must protect the secret.

```
b599de2309e31a21e41394d1614051bb4be8e2ba
```

Typically over a long period of time.

```
9b55f92f710a65aa60ac2d50fa73188831b6e77f
```

# Private and Non-Persistent

Secure Remote Password enables parties to share knowledge of a secret, without revealing the secret to the server.

…now equate credit cards as one-time shared secrets for a purchase.

…then generalize this to a search problem where terms are not revealed.

# Privacy Grabs, e.g. OAuth

User exchanges **data**, such as contacts.

User authorizes **impersonation**, such as posting messages.

Provider achieves **centralization** of a user’s activity.

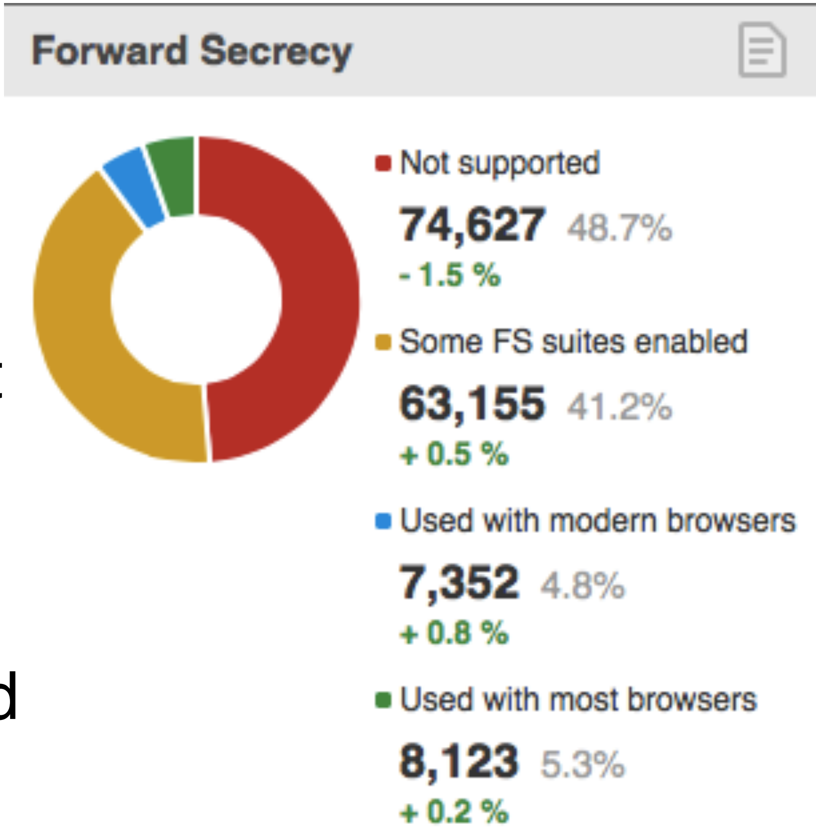
# Durational Relevance—HTTPS

Immediate positive effect against intermediation.

Impermanent effectiveness against sniffing and brute force.

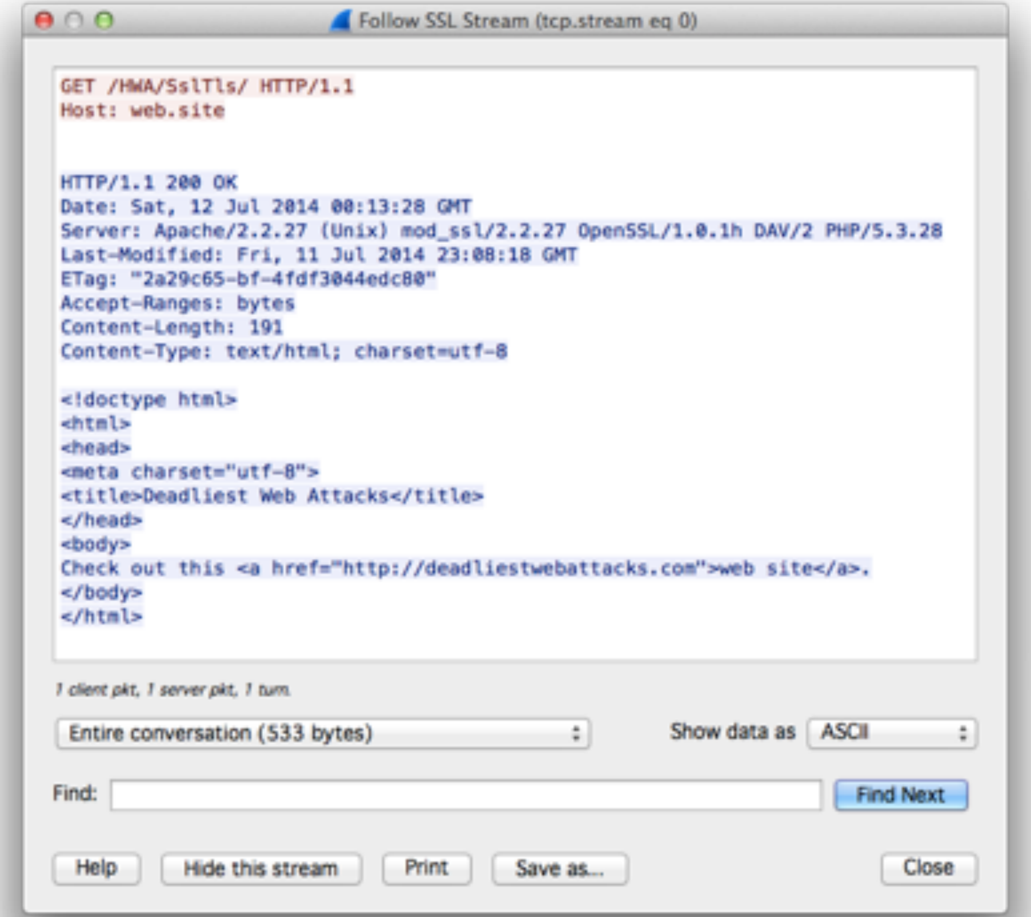
Captured traffic persists.

Cipher choice exposes captured traffic to compromised secret key.



* https://www.trustworthyinternet.org/ssl-pulse/

# Ciphers and Secrets



Follow SSL Stream (tcp.stream eq 0)

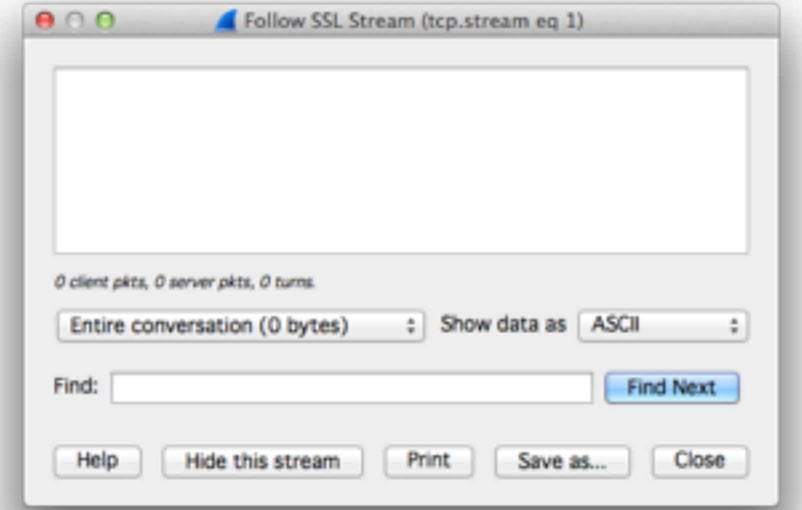
```
GET /HWA/SslTls/ HTTP/1.1
Host: web.site


HTTP/1.1 200 OK
Date: Sat, 12 Jul 2014 00:13:28 GMT
Server: Apache/2.2.27 (Unix) mod_ssl/2.2.27 OpenSSL/1.0.1h DAV/2 PHP/5.3.28
Last-Modified: Fri, 11 Jul 2014 23:08:18 GMT
ETag: "2a29c65-bf-4fdf3044edc80"
Accept-Ranges: bytes
Content-Length: 191
Content-Type: text/html; charset=utf-8

<!doctype html>
<html>
<head>
<meta charset="utf-8">
<title>Deadliest Web Attacks</title>
</head>
<body>
Check out this <a href="http://deadliestwebattacks.com">web site</a>.
</body>
</html>
```

*1 client pkt, 1 server pkt, 1 turn.*

Entire conversation (533 bytes)

Show data as ASCII

RC4-SHA



Follow SSL Stream (tcp.stream eq 1)

*0 client pkts, 0 server pkts, 0 turns.*

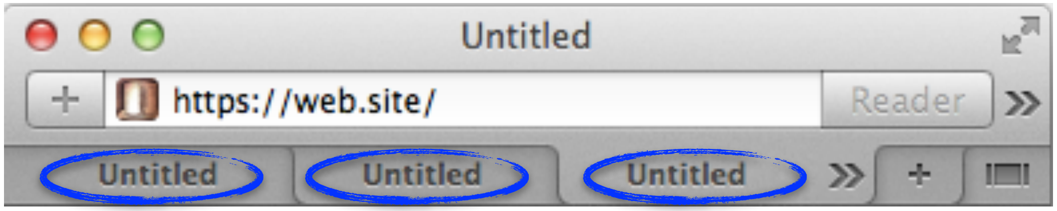
Entire conversation (0 bytes)

Show data as ASCII

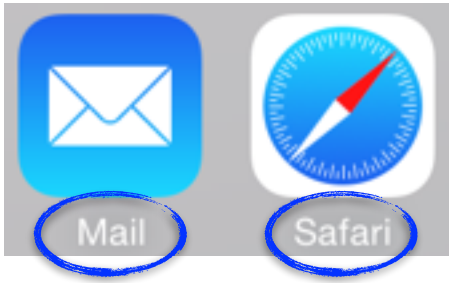
DHE-DSS-AES256-SHA

# Transport vs. Content Privacy

Browser-based email apps that attempt encryption run **unsigned code** to read **signed emails**.



Mobile apps have stronger sandboxes in terms of data isolation.



# Encryption Isn’t Perfect Privacy

Coarse fingerprinting of browsers’ default protocol/cipher choices.

Remains difficult to implement securely, e.g. BEAST, CRIME, Heartbleed, …

Does not impede traffic analysis of metadata.

# [Example] Bitcoin Blockchain

Transactions are anonymous, but not private; all are exposed and remembered by design.

Wallets can be identified, parties in transactions narrowed down.

* http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

# Mobile Device, Mobile Data

Some apps rediscovered basic security failures in misuse of HTTPS and plaintext storage on device.

Even so, app sandboxes have stronger data isolation than browsers.

Consequently, apps make more explicit data grabs.

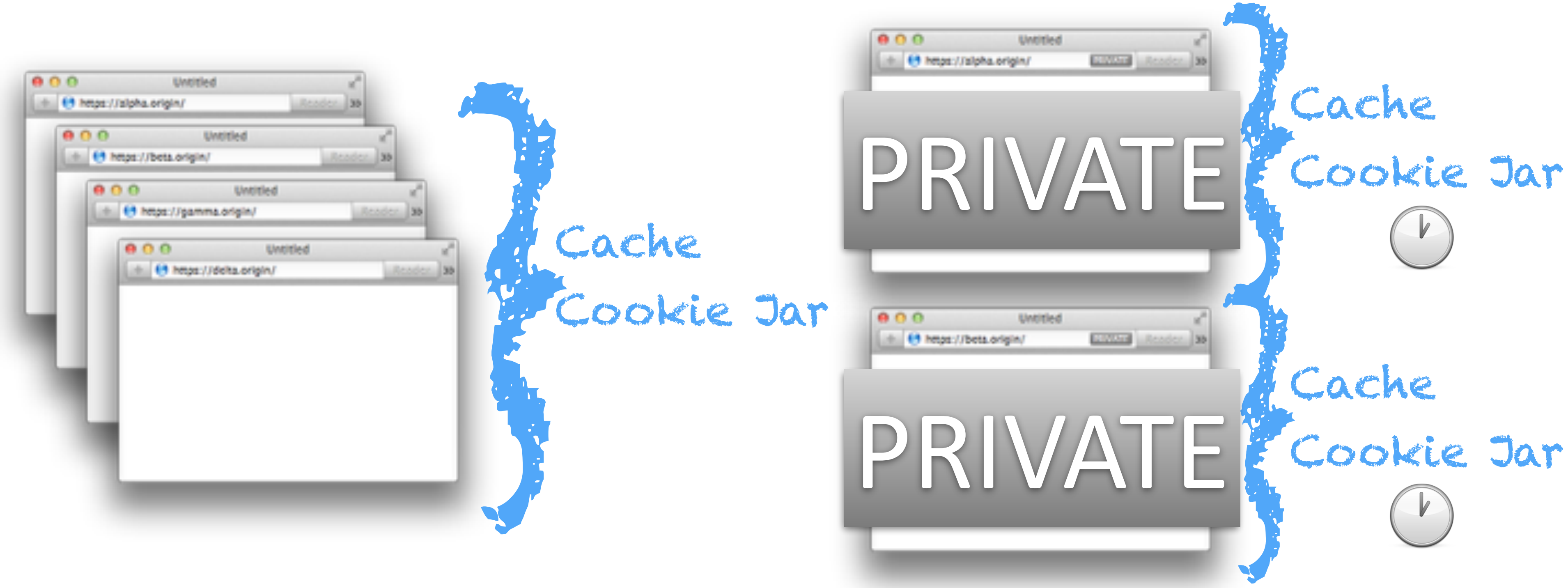
# User Agent for the Users

Establish a default strong privacy stance that echoes default security.

Expose cryptographic schemes to improve password and identity management.

Improve data isolation with “Context Vaults” and tab separation.

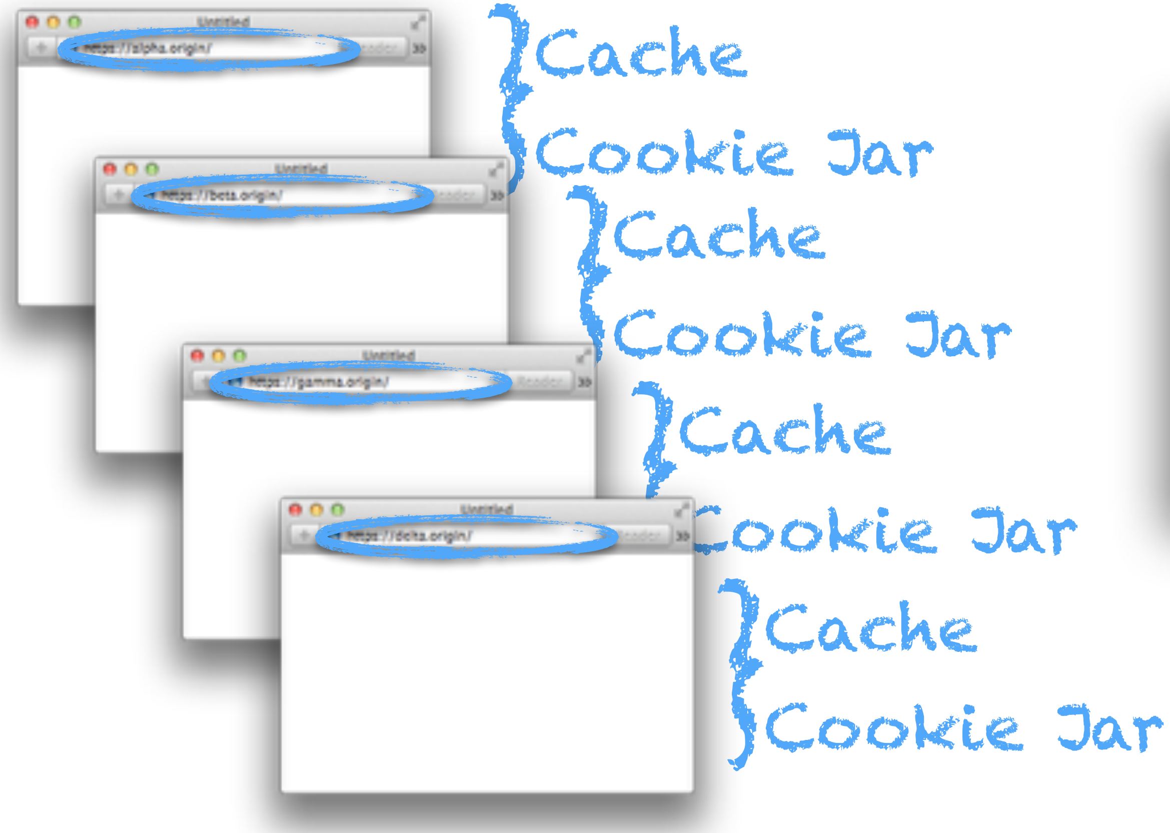
# Persistence of Vision

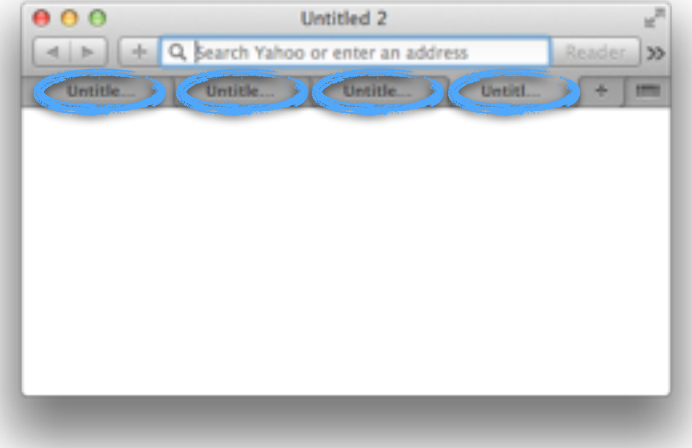


HTML5/DOM Storage
Console Messages
Application Cache
Page Search Results

Icon Database
Cache
Back/Forward Page History

# Cloistered Browsing / Context Vaults





# Protecting Data By Polluting It

“Two methods (other than recourse to ideal systems) suggest themselves for frustrating a statistical analysis. These we may call the methods of *diffusion* and *confusion*.”

- Claude Shannon, *“Communication Theory of Secrecy Systems”*. 1949.

# Diffusion

Actively pollute cookie* values in order to reduce the correlation of the tracked identity associated with it.

Pool and randomly distribute tracking values instead of (in addition to) forcing expiration.

```
_x  X1.2.815605246.1289949686 .web.site /   expiration
```

*…and beacon, pixel, etc.

# Confusion

Avoid tracking bugs in the first place.

Use canaries in anonymous, pre-auth situations, e.g. iOS 8 Wi-Fi probes and randomized MAC addresses.

# Use Your Illusion

A Tor network obfuscates identity tied to an IP address.

Create a “Rot” network that obfuscates identity tied to tracking data (via pooling, pollution).

Browsers join a Crowd as a Service model in order to distribute tracked identities.

# Some Parting Privacy Points

Personas - Independent collections of data

Protection - Default settings increase privacy, opt-in to data exposure

Penalties - Effects for willful or malicious bypass of a protection

Persistence - Settings and policies remain in effect, changes are highlighted and transparent

Pollution - Active countermeasures against tracking

# Summary

The encouragement of default secure has yet to reach default private.

Client-side data isolation needs complementary server-side controls that allow data to decay.

Establish technical controls that supplement legal and policy decisions.

# Thank You!

Slides at http://deadliestwebattacks.com

Questions @CodexWebSecurum

# References

http://beefproject.com

https://browsercheck.qualys.com

http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

http://d3js.org

https://github.com/mozilla/lightbeam

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

https://www.ssllabs.com

http://trac.webkit.org/wiki/Fingerprinting