Fixing The Internet Of Sh*t

a.k.a. “How to design secure web apps”

A presentation by Greg Slepak

at
Greg Slepak

@taoeffect

Espionage

okTurtles

GroupIncome
What
The Internet of 💩?
nice idea, but honestly i think this would make me *more* worried about the stove turning it self on

The Internet of 🖢️?

Inirv React is the first device that lets you control your stove from your smartphone and helps
Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages
Germany bans internet-connected dolls over fears hackers could target children

By Justin Huggler, Berlin
17 February 2017 • 5:02PM

Cayla doll

Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech
Watch Chinese Hackers Control Tesla's Brakes From 12 Miles Away

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

SAN FRANCISCO, CA - AUGUST 10: A Tesla Model S is displayed inside of the new Tesla flagship facility on August 10, 2016 in San Francisco, California. (Photo by Justin Sullivan/Getty Images)

Vibrator Maker To Pay Millions Over Claims It Secretly Tracked Use

March 14, 2017 - 1:52 PM ET

CAMILA DOMONOSKE

Source: http://www.npr.org/sections/thetwo-way/2017/03/14/520123490/vibrator-maker-to-pay-millions-over-claims-it-secretly-tracked-use
It’s more than that.
28 Trackers found on www.theguardian.com

26 Blocked

Resume

Trackers

Advertising
24 Trackers 23 Blocked

- Adify
- Advertising.com
- AppNexus
- BidSwitch
- BrightRoll
- Eritea
- DoubleClick
- Facebook Custom Audience
- Google Adsense
- Google AdWords Conversion
- Google Dynamic Remarketing
- Google Publisher Tags

Map These Trackers
It’s more than that.
Already, *currently*, do!

1. Injecting undetectable, undeletable tracking cookies in all of your HTTP traffic
2. Pre-installing software on your phone and recording every URL you visit
3. Snooping through your traffic and inserting ads
4. Hijacking your searches
5. Selling your data to marketers

Source: https://www.eff.org/deeplinks/2017/03/five-creepy-things-your-isp-could-do-if-congress-repeals-fccs-privacy-protections
It’s more than that.
Alt video link: https://youtu.be/7QLaKW8ABy4?t=21s
It’s more than that.
Amazon Drive Platform terms: “Don’t build apps that encrypt customer data” 😠
developer.amazon.com/public/apis/ex ...
This page is secure (valid HTTPS).

- **Valid Certificate**
  The connection to this site is using a valid, trusted server certificate.
  [View certificate]

- **Secure Resources**
  All resources on this page are served securely.

- **Public-Key Pinning**
  Public-key pinning was bypassed by a local root certificate.

---

**Greg Slepak** @taoeffect · 4 Jul 2016

This is @ChromiumDev’s idea of “showing people they’re being MITM’d”:
bugs.chromium.org/p/chromium/iss... pic.twitter.com/NKdAbUbNjP
Sigh. TLS 1.3 temporarily turned off in Chrome Stable because of intercepting proxies.

[Link to bug report]

---

**BlueCoat and other proxies hang up during TLS 1.3**

**Project Member**  Reported by [jayhlee@google.com](mailto:jayhlee@google.com), Feb 21

Chrome Version: 56  
OS: Chrome and Windows

**What steps will reproduce the problem?**

1. BlueCoat 6.5 proxy.  
2. Chrome OS 56 or Chrome browser 56  
3. Attempt to connect to a Google service (youtube, accounts.google.com, etc).

**What is the expected result?**

Successful connection. Client and proxy may negotiate down to TLS 1.2 instead of TLS 1.3.

**What happens instead?**

When Chrome attempts to connect via TLS 1.3, BlueCoat hangs up connection.

---

Source: [Twitter](https://twitter.com/FiloSottile/status/835269932929667072)
Source: [Chromium bug](https://bugs.chromium.org/p/chromium/issues/detail?id=694593)
Blue Coat

American Company Blue Coat, specialized in online security, is best known for its Internet censorship equipment. This equipment also allows for the supervision of journalists, netizens and their sources. Its censorship devices use Deep Packet Inspection, a technology employed by many western Internet Service Providers to manage network traffic and suppress unwanted connections.

The Company

Country of origin: USA
Website: www.bluecoat.com

Blue Coat is a large IT company based in Sunnyvale, California, that is best known for providing filtering and censorship devices for countries such as Syria and Burma. The company also provides network analysis systems called "Intelligence Centres," which are used by companies and governments to monitor online traffic and identify performance problems. They allow for the monitoring of individual online behaviour.

They're listening to this company. Not you.
Compromising your home Internet connection to secretly spy on employees.
Sounds about right: "Google has officially vertically integrated the Internet."

You can now have a website secured by a certificate issued by a Google CA, hosted on Google web infrastructure, with a domain registered using Google Domains, resolved using Google Public DNS, going over Google Fiber, in Google Chrome on a Google Chromebook. Google has officially vertically integrated the Internet.
Study shows Google may influence how you vote


The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections

Robert Epstein¹ and Ronald E. Robertson
@google appears to be manipulating the election: youtube.com/watch?v=PFxFRq… HT @SourceFed
This video is unavailable.

Sorry about that.
“Sorry about that.”
Speaking of censorship...
BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA

BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA

sal
@tevet

Found another 'unfollow' that I DID NOT UNFOLLOW --->
@Ayaan Nor would I have done. Added to list try to prevent
#Twitter #Censorship antics

4:38 PM - 18 Jun 2016

↩️ 2  ❤️ 2
BUSTED! Twitter Caught Manipulating Tweets Of Former BlackRock Fund Manager Critical Of CIA and NSA

Was wondering why you stopped tweeting until I realized tweet unfollowed you automatically. I thought that sorta stuff was a bit tin foil hat but it's as real as can be.

2:03 PM

Thanks! I hear this every day. Have heard it hundreds of times.

2:09 PM
How often does this happen to your tweets?
fixingtao.com/other/images/t ... 

0% 1/week or more
0% 1/month or more
17% all the time
83% never?

6 votes • Final results
Greg Slepak
@taoeffect

Have you noticed tweet notifications automagically disappear / get cleared on your device's lock screen by themselves?

19% I've paid attention, & Y
25% I've paid attention, & N
56% I haven't paid attention

16 votes • Final results
Twitter apparently deleting people's tweets now.

AJ Joshi @AJ
@taoeffect I didn't delete that (from memory) it was disconnected
“Bugs”?
The “Internet of Sh*t” is “The Internet”
...ok.

... what happened to “fixing it”?
A better question is:

Do you want to fix it?
Raise your hand if you want this fixed
Raise your hand if you would help fix this

(if you could)
Who wants change?

Who wants to change?
Before we start, a few inspirational quotes

:-)
“Be the change you want to see in the world.”

“Insanity is doing the same thing over and over and expecting a different result.”

“80% of solving a problem is understanding it.”

so… you’re 80% there already???
Break Down The Problem
Into Manageable Pieces
1. Economic

2. Technological
Economic
Invest in solutions instead of problems
Invest in decentralization

And use small(er) VPS providers
Brave

63,198 Trackers Blocked
9,971 Ads Blocked
19,587 HTTPS Upgrades
2 hours Estimated Time Saved
Explore new economic systems

GroupIncome

Patreon
Technological
The decentralization of a system can be measured.

Deconfusing

Decentralization

A 5 Minute Talk for DEVCON1 by Greg Slepak

Alt video link: https://www.youtube.com/watch?v=7S1IqaSLrq8
Centralized systems are **incapable** of censorship-resistance.

2. **Architecture is fully decentralized.**

Screenshot of the 3rd “Short” here: [https://groupincome.org/shorts/](https://groupincome.org/shorts/)
Last time...

Zooko's Triangle

“Decentralized Consensus-based Namespaces”
A “decentralized consensus-based namespace” provides **censorship-resistance** and **user-owned and controlled identities**
Answer: DPKI

That means security.
Decentralized Public Key Infrastructure

A White Paper from Rebooting the Web of Trust

by (alphabetical by last name) Christopher Allen, Arthur Brock, Vitalik Buterin, Jon Callas, Duke Dorje, Christian Lundkvist, Pavel Kravchenko, Jude Nelson, Drummond Reed, Markus Sabadello, Greg Slepak, Noah Thorp, and Harlan T Wood

Abstract

Today’s Internet places control of online identities into the hands of third-parties. Email addresses, usernames, and website domains are borrowed or "rented" through DNS, X.509, and social networks. This results in severe usability and security challenges Internet-wide. This paper describes a possible alternate approach called decentralized public key infrastructure (DPKI), which returns control of online identities to the entities they belong to. By doing so, DPKI addresses many usability and security challenges that plague traditional public key infrastructure (PKI). DPKI has advantages at each stage of the PKI life cycle. It makes permissionless bootstrapping of online identities possible and provides for the simple creation of stronger SSL certificates. In usage, it can help “Johnny” to finally encrypt thanks to its relegation of public key management to secure decentralized datastores. Finally, it includes mechanisms to recover lost or compromised identifiers.

Source: https://blog.okturtles.com/2016/02/turtle-status-letter-1-browser-extension-dnschain-dpki-more/#DPKI
# Comparison

<table>
<thead>
<tr>
<th></th>
<th>Google’s CT</th>
<th>Google’s KT</th>
<th>CONIKS</th>
<th>DPKI</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITM-detection</td>
<td>😞</td>
<td>😞</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>MITM-prevention</td>
<td>✗</td>
<td>✗</td>
<td>✅(*)</td>
<td>✅</td>
</tr>
<tr>
<td>Internet scalable</td>
<td>✅</td>
<td>✅</td>
<td>✅</td>
<td>😞</td>
</tr>
<tr>
<td>Economically backed security</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>Censorship resistant</td>
<td>😞</td>
<td>✗</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>DoS resistant</td>
<td>✅</td>
<td>😞</td>
<td>😞</td>
<td>✅</td>
</tr>
</tbody>
</table>

[https://blog.okturtles.com/2017/02/coniks-vs-key-transparency-vs-certificate-transparency-vs-blockchains/](https://blog.okturtles.com/2017/02/coniks-vs-key-transparency-vs-certificate-transparency-vs-blockchains/)
Potential Partial Implementations

uport

Blockstack
DCS / Slepkak’s Triangle
We observe that any single system may possess, at most, two of three properties:

- **Consensus** means the system has participants who regularly come to agreement about changes to the system’s shared state (shared resource). The interval at which the system comes to agreement is its *period*, $\pi$.

- **Mainstream** (or **Scalable**) means the system is, *by itself*, capable of competing with the transactional demands placed on a leading centralized competitor.\(^1\)

- **Decentralized** means the system meets two related notions of *decentralization*:

\(^1\)For example, we could compare Bitcoin’s transaction rate to VISA’s, or BitTorrent’s ability to stream movies to Netflix.
Recap
Avoid centralized systems

(when possible, but especially for key management)
Use + support + design decentralized systems
Questions?

Decentralize All The Things!

- uport
- GroupIncome
- Patreon
- okTurtles
- blog.okturtles.com
- Blockstack
- IPFS
- Bitcoin
- Ethereum
- ZeroNet