5 CRAZY FUTURE SECURITY STIMULI

Joseph Lorenzo Hall, https://cdt.org/

NSPW Sep-2016

Introduction

- Me: Former pizza maker, pastry chef, ranch worker (yoga, riflery, lifeguard), astrophysicist, voting machine hacker
  … ***probably best to think of me as ½ lawyer, ½ computer scientist***
- CDT: Non-profit digital rights organization, focus on research and advocacy
  - *Support: foundations, companies, cypres/donations*
  - *Principles:*
    - The internet empowers people
    - Forward-looking, collaborative solutions
    - Tangible, pragmatic policy outcomes
- Some of what we do is never public

Quick examples of my work

- Building human rights values into core internet infrastructure
- Working to protect as much traffic as possible, “HTTPS evangelism”

Quick exam

- Building human right
- Working to protect as

CENTER FOR DEMOCRACY & TECHNOLOGY

Sep 2016

Issue Brief: The Time Has Come to Move to HTTPS!

All Web Users Deserve Confidentiality and Integrity:

All interactions on the Web benefit from prot
financial fraud to spying and surveillance to m
protection is achieved by HTTPS, and now is t
(secure) HTTPS. It's easier than you may think

Privacy & Security Concerns of not using HTTP

➢ **Without HTTPS, ISPs and governments can sp**
traverses many different networks from serve
installed on those networks) can see the full c
your web traffic to
nencrypted traffic
tic since the US gov
m the restrictions i
ffic travelling from
sily cross internatio

[Docs] [txt|pdf|xml|html] [Tracker] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01 02 03 04

Network Working Group — J. Hall
Internet-Draft — CDT
Intended status: Informational — M. Aaron
Expires: January 9, 2017 — CU Boulder
B. Jones
N. Feamster
Princeton
July 08, 2016

A Survey of Worldwide Censorship Techniques
draft-hall-censorship-tech-04

Abstract

This document describes the technical mechanisms used by censorship regimes around the world to block or impair Internet traffic. It aims to make designers, implementers, and users of Internet protocols aware of the properties being exploited and mechanisms used to censor end-user access to information. This document makes no suggestions on individual protocol considerations, and is purely informational, intended to be a reference.

Title: It's Time to Move to HTTPS! (Yes, even the naughty bits)
Author: Greg Norcie

You've heard us talk extensively about the importance of moving encrypted version of the Web's HTTP protocol.

Today, CDT is releasing a one-pager aimed for website system a bosses!) that describes the importance of HTTPS. (You should be out out for anyone that thinks HTTPS is no big deal. It's a big dea

The very short version of our argument:

- Without HTTPS, ISPs and governments can spy on what
- Using HTTPS prevents malicious actors from injecting ma
- You already need HTTPS to do payments if you accept m
- Without HTTPS, ISPs can strip out your ads/referrals and
- Without HTTPS your website cannot utilize HTTP/2 for op
- Without HTTPS, you can't use the latest web features tha geolocation)
- Without HTTPS, you can't can't know if your users receive your terms of service and privacy policy without modificati

Wider Software Independence?

- In voting technology work, we've had a notion of Software Independence:

  "A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome." (Wack, Rivest 2008)

- We do this now with a paper trail and audits… grounding logs in physical matter
- Out-of-band mechanisms and hardware security components ground trust in physical matter, what about forensic logging on physical matter?
- This seems more widely useful, especially in transaction-like critical infrastructure
- What would it look like? Jones: etched alluminum. Molecular fixation?

Security Infrastructure Sustainability?

- Heartbleed, Shellshock
- Core Infrastructure Initiative, Mozilla Open Source Support program (stop gaps!)
- How can we fix this more permanently?
- Crazy idea? What about treating security primitives as a ”security commons”?
  - *Basic idea is to create a “physics” of security*
  - *Monoculture doesn’t seem as dangerous if we are all “all in”*
  - *Can concentrate resources in a few important areas*
  - *The result should be more common attack surface, more standard expectation of level of protection*

Privacy in Cognitive Computation?

- Governments equate computerization with mandating *accessibility* and *modifiability*
  - *Apple v. FBI, WhatsApp in Brazil, etc.*
- However, we've "always accepted limits in detecting bad people doing bad things in open societies" (Chertoff)
- Further, Democracy itself requires people to have the freedom to think in private
- What are the limits of government reach when we have computational cognitive support systems? Is there a future where we can no longer keep "hard secrets"?
  - *Can we secure these systems against the ultimate adversaries (governments)?*
  - *Can legal rules set bright lines for subpoenaing information from inside our heads?*

Security Development in the Shadows?

- There are powerful forces pushing against end-to-end security mechanisms
  - *E.g., The UK IPB and extraterritorial design mandates for cleartext*
- This may be impossible for industry to combat…
  - *Apple, Microsoft, Google, Cisco, Facebook, etc. unlikely to pull out of those markets*
  - *The concentration of tech companies in the US means little political empathy*
- Most direct effect: much harder to provide *usable* security *by default*
- Much more difficult to compel open source or anonymous development
  - *Will core security tools be developed increasingly by open source consortia?*
  - *Do we see a future in which strong security mechanisms have to be developed in the shadows? Essentially like terrorist/spycraft cells?*

Security in a Research Singularity?

- Technological singularity is often associated with superintelligence
- Softer notions of a singularity, especially in active research fields
  - *It is not hard to see a time where research is so intense that we cannot communicate research results quickly enough to incorporate into ongoing work*
- How does security research – applied or fundamental – operate in this kind of environment?
  - *Do we need models where we're always operating on stale information?*
  - *How do we avoid adversaries leveraging highly heterogeneous threat information?*
  - *Does this regress to having no/little communication? (Medieval castles)*