Privacy Isn't Dead

•••

Stephen Smith
2017-01-29

What Are We Going To Talk About Today?

Who Are You, And Why Are You In My Conference?

Status Quo

Secure Alternatives

How They Work

Where To Get Them

Closing Thoughts

Who are you, and why are you in my conference?

Stephen Smith

Backend Developer / DBA / Security Freak at REDspace
 - we're hiring (http://redspace.recruiterbox.com)

Fervent believer that privacy is not dead

Two Disclaimers

Disclaimer #1

I am not a professional operational security consultant

If you think the government is after you, talk to someone else

But this talk is pretty good for most people

Disclaimer #2

“If you have nothing to hide you have nothing to fear” is not an excuse

The future can be much different

Hollywood pre and post McCarthy era

LiveJournal pre and post Russian ownership

Alright, let’s get on with the show

Status Quo

Web Browsing

Traffic monitoring

Traffic logging

Regional censorship

Email

Can still be monitored and logged

Can also be modified en route, on server, or falsified entirely

Can be hacked and disseminated to the world at large
- Luckily nobody's interested in that

Text Messages and Phone Calls

Still monitoring and logging

Passwords

Too short

Repeated across websites

Written on sticky notes and carefully hidden underneath keyboards

Secure Alternatives

Secure Alternatives

Web browsing = Tor

Text messages and phone calls = Signal

Email = PGP (or Signal)

Passwords = password manager

How They Work

Why should I care how they work?

Black boxes are death

Kerckhoff's Principle

Schneier's Law

How Tor Works

Tor = The Onion Router

Data to relay node

Relay node marks packet, cycles

Packet eventually reaches exit node

And then back again

(this is the conference-speech-size explanation)

How Signal Works

Signal app VS Signal Protocol

WhatsApp, Facebook Messenger, Google Allo

Signal app keeps very little data about you

Signal protocol *“combines the Double Ratchet Algorithm, prekeys, and a triple Diffie-Hellman handshake. It uses Curve25519, AES-256, and HMAC-SHA256 as primitives.”*
- aka “Good Things” (fun research project if you want to learn more)

I’ve used it for about a year now, no complaints

How Things Can Not Work (in order of severity)

MITM, or Man In The Middle
- can be ameliorated through the Socialist Millionaire Problem (such a great name)

Side Channel Attack
- attacks on implementation, not on theory (e.g. WhatsApp key verification)

Actual Mathematical Flaw
- only happens a time or two a decade
- hopefully you've already stopped using the thing

Consider the source

Thoroughly research any product that claims to protect your privacy

Hall of Shame = Cryptocat, Hushmail, Telegram

Hall of Fame = Tor, Signal

How To Use Them

How To Use Tor

Windows/Mac/Linux = Tor Browser Bundle

Android = Orbot + Orfox

iOS = Onion Browser

How To Use Signal

Install it

¯_(ツ)_/¯

How To Use A Password Manager

Multiple options, all work essentially the same way

On-disc VS Cloud

Password Safe

LastPass

Dashlane

2FA w/YubiKey?

Bonus Round: Passwords VS Fingerprints

THIS IS NOT LEGAL ADVICE PLEASE TALK TO YOUR LAWYER

However...

s.13 of CCRF (can’t be compelled to disclose contents of mind)

Fingerprints = case by case basis. Do you feel lucky?

Either is better than neither

Closing Thoughts

Closing Thoughts

Most modern communication is as secure as screaming out a window

There are alternatives

Don’t call me if you get arrested

TL;DR

Edward Snowden ✓
@Snowden

Follow

Use Tor. Use Signal.

> **AI96** @Hitsmanalex
> @Snowden @verge what message service should i use

RETWEETS 1,787 LIKES 2,567

6:50 AM - 21 Sep 2016

1.8K 2.6K

Questions?

...

steve@rzw.ca

Slides available at http://HireSteve.ca/Podcamp2017.pdf