Secure Communication

Hacking/Hustling Workshop @ Eyebeam

t4tech

About me

Liz!

She/Her

Electrical Engineer/Embedded developer

Teaching for a while

Overview

Signal is one example of a third-party app for secure texting.

We’ll go over what it does and why it’s important.

We’ll install it.

We might get to protonmail.

We might get to PGP.

Insecure Texting

SMS/MMS

Short Message Service and Multimedia Message Service

Insecure Texting

Texts are relayed through “Short Message Service Centers” which store and attempt to forward message to recipient.

Insecure Texting

SMS/MMS is unencrypted.

You do not have control over which Short Message Service Center your text goes through.

You do not have control over what that center does with your text.

What to do

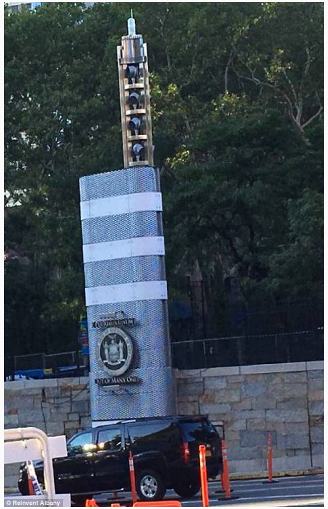
There are several insecurities in standard texting.

I will break it down into types of general attacks, and show how Signal addresses these attacks.

Refer to your threat models.

Listening Attack

An attacker on an untrusted network listens in on your conversation.



© Reinvent Albany

Listening Attack: Defense

A: Don’t use untrusted networks

Listening Attack: Defense

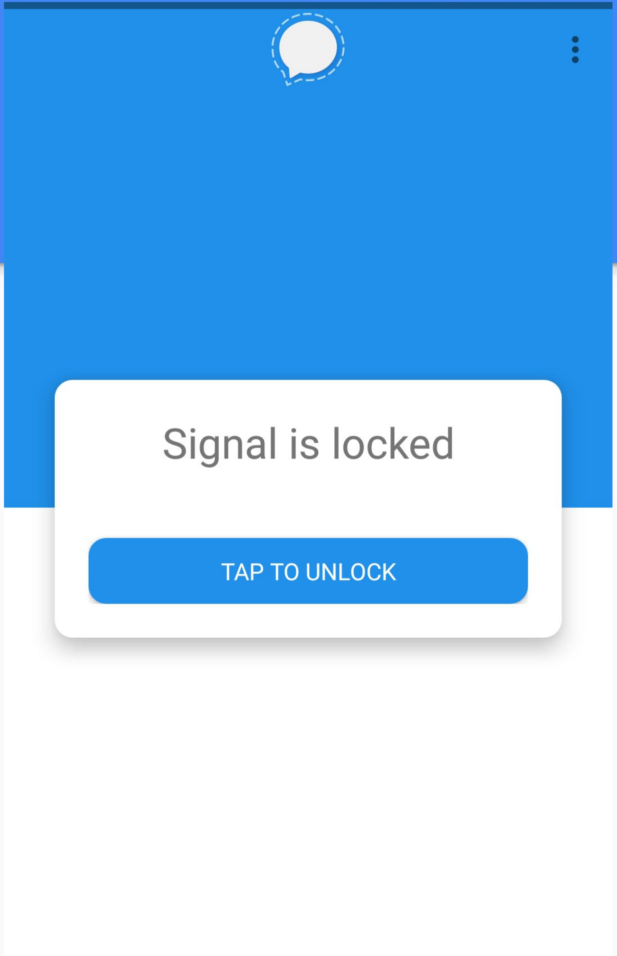
B: Use encryption - Signal

Physical Attack

An attacker has physical access to your device.

Physical Attack: Defense

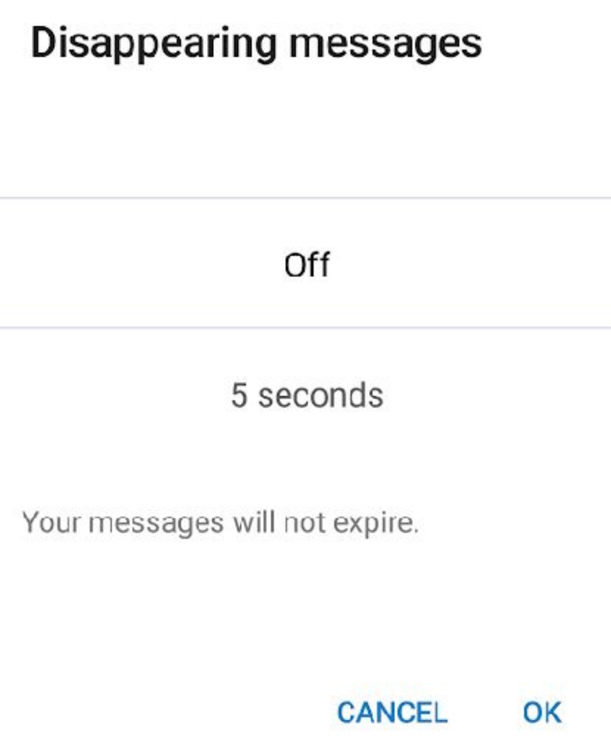
A: Use a password



Signal is locked

Physical Attack: Defense

B: Use Disappearing messages



Disappearing messages

Off

5 seconds

Your messages will not expire.

Person in the Middle Attack

An attacker impersonates the person you are trying to talk to.

Or

An attacker impersonates you.

Person in the Middle Attack: Defense

A: Encryption keys

Person in the Middle Attack: Defense

B: Registration PIN

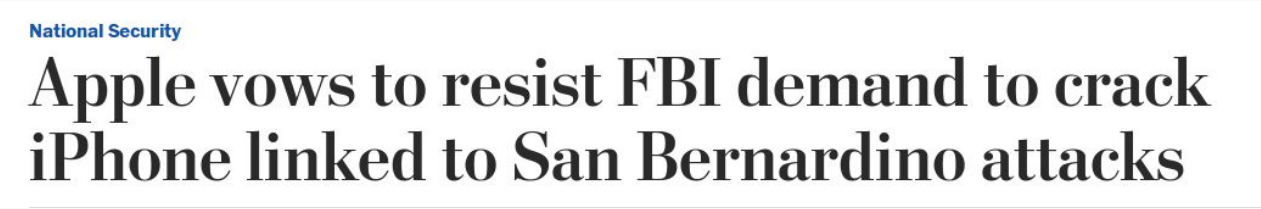
Install Signal

Third Party Apps

Open Source vs Proprietary

Third Party Apps

Server location



National Security

Apple vows to resist FBI demand to crack iPhone linked to San Bernardino attacks

Third Party Apps

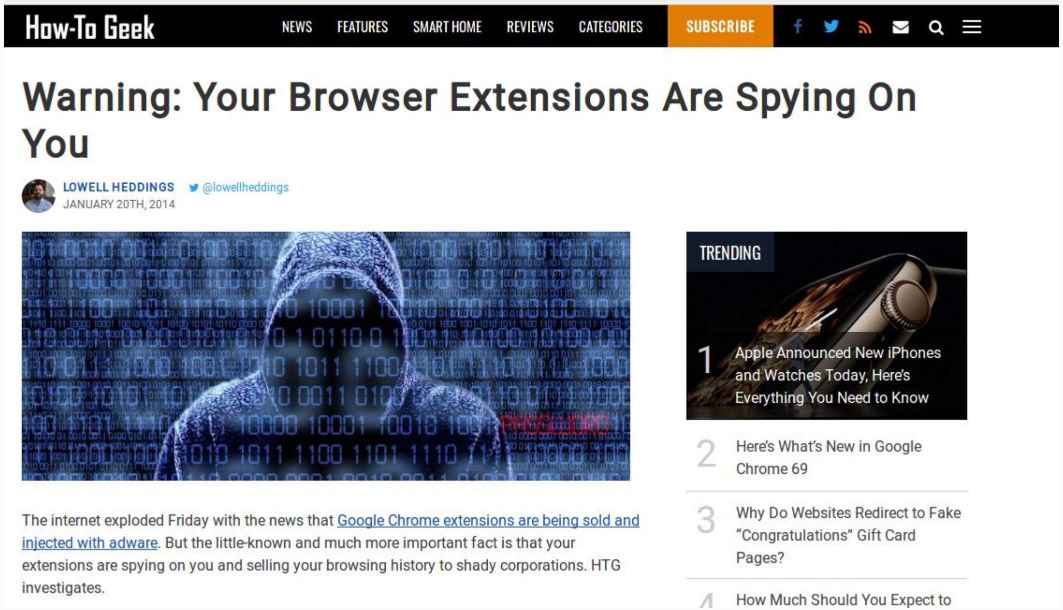
Trusted Provider

Third Party Apps

Common usage and your threat model

Trusted provider and OS

Person in the Mi



Warning: Your Browser Extensions Are Spying On You

LOWELL HEDDINGS @lowellheddings
JANUARY 20TH, 2014

The internet exploded Friday with the news that Google Chrome extensions are being sold and injected with adware. But the little-known and much more important fact is that your extensions are spying on you and selling your browsing history to shady corporations. HTG investigates.

TRENDING

1 Apple Announced New iPhones and Watches Today, Here's Everything You Need to Know

2 Here's What's New in Google Chrome 69

3 Why Do Websites Redirect to Fake "Congratulations" Gift Card Pages?

4 How Much Should You Expect to

Email

Similar to SMS, however goes across Internet Service Providers

Insecure Email

Email is generally unencrypted, and is vulnerable to person in the middle attacks.

Protonmail

protonmail.com

Encrypts communication between protonmail emails.

Protonmail

Servers hosted in Switzerland

Install Protonmail

Some Language

End-to-End Encryption

Zero Access Encryption

Some Language

TLS - Transport Layer Security

PGP

“Pretty Good Privacy”

openpgp.org

Requires both parties to use PGP

OpenPGP example

t4tech