Privacy & Security Resources

Guides

- AnonymousPlanet - anonymousplanet.org

  > This is a maintained guide with the aim of providing an introduction to various online tracking techniques, online ID verification techniques, and detailed guidance to creating and maintaining (truly) anonymous online identities. It is written with hope for activists, journalists, scientists, lawyers, whistle-blowers, and good people being oppressed, censored, harassed anywhere! This guide has no affiliation with the Anonymous collective/movement.

- PrivacyGuides - privacyguides.org

  > Privacy Guides is a non-profit, socially motivated website that provides information for protecting your data security and privacy.

- Advanced Privacy and Anonymity Using VMs, VPN’s, Tor - ivpn.net

  > If you’re here, you may be using (or considering) a VPN service to provide online privacy and anonymity, and perhaps to circumvent Internet censorship. This series of guides goes far beyond that. It explains how to obtain vastly greater freedom, privacy and anonymity through compartmentalization (aka compartmentation) and isolation, by using multiple virtual machines (VMs) with Internet access through nested chains of VPNs and Tor.

- How to create anonymous Telegram and Signal accounts without a phone

  > This guide (Whonix + Anbox) also works for other apps, such as Signal, Samourai Wallet, Schildi Chat and more.

- AnonymousLand - anonymousland.org

Android

- A brief and informal analysis of F-Droid security - Wonderfall.dev

  > F-Droid is a popular alternative app repository for Android, especially known for its main repository dedicated to free and open-source software. F-Droid is often recommended among security and privacy enthusiasts, but how does it stack up against Play Store in practice? This write-up will attempt to emphasize major security issues with F-Droid that you should consider.

- Android Tips - PrivSec.dev

  > Android is a very secure and robust operating system out of the box. This post will be less of a “hardening guide”, but more of a non-exhaustive list of tips when it comes to buying and using Android phones.

- Android - madaidans-insecurities.github.io

  > this article explains common ways in which people worsen the security model rather than criticisms of the security model itself.

- EOF

Desktop

- Desktop Linux Hardening - PrivSec.dev

  > The goal is to produce a guide that intermediate to advanced Linux users can reasonably follow to set up and maintain the security configurations. It will also not try to be distribution agnostic, and there will be many distribution specific recommendations.

- Linux - madaidans-insecurities.github.io

  > Linux being secure is a common misconception in the security and privacy realm. Linux is thought to be secure primarily because of its source model, popular usage in servers, small userbase and confusion about its security features. This article is intended to debunk these

> misunderstandings by demonstrating the lack of various, important security mechanisms found in other desktop operating systems and identifying critical security problems within Linux’s security model, across both user space and the kernel. Overall, other operating systems have a much stronger focus on security and have made many innovations in defensive security technologies, whereas Linux has fallen far behind.

- Linux Hardening Guide - madaidans-insecurities.github.io

  > “Linux is not a secure operating system. However, there are steps you can take to improve it. This guide aims to explain how to harden Linux as much as possible for security and privacy. This guide attempts to be distribution-agnostic and is not tied to any specific one.

- Choosing Your Desktop Linux Distribution - PrivSec.dev

  > “Not all Linux distributions are created equal. When choosing a Linux distribution, there are several things you need to keep in mind.

- security-misc - kicksecure.com

  > “security-misc: Enhance Miscellaneous Security Settings

- The Linux Security Circus: On GUI isolation - blog.invisiblethings.org

  > “There certainly is one thing that most Linux users don’t realize about their Linux systems… this is the lack of GUI-level isolation, and how it essentially nullifies all the desktop security.

- Re: X11 -> Root? (Qubes square rooted) - seclists.org/dailydave

Tor and VPNs

- VPN - a Very Precarious Narrative - overengineer.dev

  > “The popularity of those services and the way they are recommended and promoted is bad. So bad that I feel impelled to write this article on it, to explain two problematic points. Those are:

> In most circumstances, VPNs do very little to enhance your data security or privacy unless paired with other changes.

> Acting as they do, and promoting commercial VPN providers as a solution to potential issues does more harm than good.

- Commercial VPN Use Cases - PrivSec.dev

  > Virtual Private Networks are a way of creating a protected and private network over the open Internet. It was originally designed to provide remote access to an internal corporate network. However, in recent years, it has also been used by commercial VPN companies to hide their clients’ real IP address from third-party websites and services.

- Don’t use VPN services - gist.github.com/joepie91

  > No, seriously, don’t. You’re probably reading this because you’ve asked what VPN service to use, and this is the answer.

  > Note: The content in this post does not apply to using VPN for their intended purpose; that is, as a virtual private (internal) network. It only applies to using it as a glorified proxy, which is what every third-party “VPN provider” does.

- You want Tor Browser … not a VPN - matt.traudt.xyz

  > (in most cases) …Tor (thus Tor Browser) is in fact built correctly to disallow anyone from ever intercepting and reading the traffic between you and your guard relay. If your chosen VPN isn’t (good luck figuring it out), then Tor (Browser) is better. But honestly, your VPN is probably just as good.

- IPVanish “No-Logging” VPN Led Homeland Security to Comcast User - torrentfreak.com

  > IPVanish, a VPN provider that for years claimed a strict no-logging policy, led Homeland Security to a suspect using a Comcast IP address, court papers filed in 2016 reveal.

- Is Tor Trustworthy and Safe? - restoreprivacy.com

> There is a lot of misinformation being promoted in various privacy circles about Tor. This article will examine some facts about Tor and assess whether it is the infallible privacy tool it's made out to be by some.

- EOF

General

- Security and Privacy Advice - madaidans-insecurities.github.io
- A Few Thoughts on Cryptographic Engineering - blog.cryptographyengineering.com

  > I'm going to devote this post to providing the world's simplest explanation of why, in the threat model of your typical journalist, your desktop machine isn't very safe. And specifically, why you're safer using a modern mobile device — and particularly, an iOS device — than just about any other platform.

- Despite DoH and ESNI, with OCSP, web activity is insecure and not private - blog.seanmcelroy.com

  > Certificate Transparency (CT) logs increasingly provide virtually every TLS certificate to be identified by serial number. Since OCSP responses are unencrypted and contain the serial number of the certificate as can be found in CT logs, as well as unsalted hashes of the certificate's Distinguished Name and public key, these can easily be profiled to compromise the privacy of clients even in the presence of DoH and ESNI privacy protections.

- Badness Enumeration - PrivSec.dev

  > Badness enumeration is the concept of making a list of known bad actors and attempting to block them. While it seems intuitive at first glance, badness enumeration should not be relied on for privacy or security. In many cases, it actually does the exact opposite and directly harms the user. This post will attempt to explain why badness enumeration as a concept is flawed and give some examples of its failings in practice.

- The Six Dumbest Ideas in Computer Security - ranum.com

> why are we spending all this time and money and still having problems?

- Threat Modeling - privsec.dev

  > “The first task a person should do when taking steps to protect their privacy and security is to make a threat model.

- The right thing for the wrong reasons: FLOSS doesn’t imply security - seirdy.one

  > “It’s no secret that I’m a passionate supporter of software freedom: I’ve written two posts about how Free, Libre, and Open-Source software (FLOSS) is necessary but insufficient to preserve user autonomy

- FLOSS Security - PrivSec.dev

  > “While source code is critical for user autonomy, it isn’t required to evaluate software security or understand run-time behavior.

  > “One of the biggest parts of the Free and Open Source Software definitions is the freedom to study a program and modify it; in other words, access to editable source code. I agree that such access is essential; however, far too many people support source availability for the wrong reasons. One such reason is that source code is necessary to have any degree of transparency into how a piece of software operates, and is therefore necessary to determine if it is at all secure or trustworthy.

- Two types of privacy - seirdy.one

  > “Threat modelling provides important context to security and privacy advice. Measures necessary to protect against an advanced threat are different from those effective against unsophisticated threats. Moreover, threats don’t always fall along a simple one-dimensional axis from “simple” to “advanced”.

- Recovering redacted information from pixelated videos - positive.security

> Information that has been redacted is often the most interesting. It’s therefore no wonder that some people might have a motivation to try to reverse such a redaction for various reasons.

> “In this blog post, I’ll discuss image/video blurring methods and their weaknesses and present a simple yet effective method to get a high-resolution image from a pixelated video in order to recover redacted information (with no guessing involved).

- Let’s Enhance! How we found @rogerkver’s $1,000 wallet obfuscated private key - medium.com/free-code-camp

  > “Last week France 2 broadcasted a documentary about Bitcoin. They interviewed @rogerkver who decided to offer $1000 in Bitcoin to the quickest viewer. Unfortunately, the QR code and the private key were obfuscated by France 2.

- Wounded QR codes - datagenetics.com

  > “QR codes store data in two dimensions in the form of an array of contrasting regions. The information density of a QR code is much higher than a vanilla barcode; depending on the format used and the resolution of reader, over a thousand bytes can be encoded in a region the size of a postage stamp.

  > “QR codes use a Reed–Solomon error correction based technology to help recover from errors in reading (for instance, caused by a smudge, badly printed code or other deformity).

- Email (In)security

  > “There is no such thing as secure email. Email is an inherently insecure protocol, conceived at a time when security was an afterthought. There are fundamental flaws with email that cannot be mitigated by slapping encryption on top.

- EOF

Fingerprinting Articles

- NetworkManager Minor Hardening - wanderingcomputerer.gitlab.io

  > MAC address randomization, Removing static hostname to prevent hostname broadcast, disabling sending hostname to DHCP server

- How CSS Alone Can Help Track You - matt.traudt.xyz

  > A common question people ask when they first start using the Tor Browser Bundle is “why does the browser recommend I don’t change my window size?” Reasonable question. And if you disable JavaScript, you may think that’s enough to make window size irrelevant. Not quite.

- Browser Tracking - madaidans-insecurities.github.io

  > Many common methods of preventing browser tracking are ineffective. This article goes over misguided ways in which people attempt to improve their privacy when browsing the web.

- Don’t update NTP – stop using it - blog.hboeck.de

  > Today several severe vulnerabilities in the NTP software were published. On Linux and other Unix systems running the NTP daemon is widespread, so this will likely cause some havoc. I wanted to take this opportunity to argue that I think that NTP has to die.

- EOF

Fingerprinting Tests

- TorZillaPrint - arkenfox.github.io

  > TorZillaPrint (TZP) aims to provide a comprehensive, all-in-one, fingerprinting test suite, nicely broken into suitable sections with relevant information together. Long term, the goal is to collect Gecko only fingerprint data (no PII) for analysis to see how many classifications each metric or section provides.

- No-JS fingerprinting - noscriptfingerprint.com

> A common misconception is that disabling JavaScript can prevent fingerprinting. Since advertisers and bad actors use it for ad targeting and tracking your online activity, it’s a natural (albeit incorrect) assumption that disabling JavaScript will protect you against fingerprinting. In this article, we will demonstrate that fingerprinting can occur even in the absence of JavaScript.

- CSS Fingerprint - csstracking.dev

  > CSS Fingerprinting is a technique of tracking and gathering information on site visitors. This method exploits the nature of CSS to collect various characteristics about the visitor’s browser and device, which can later be used to either identify or track said visitor.

- CreepJS - abrahamjuliot.github.io

  > Creepy device and browser fingerprinting

- Kloak - whonix.org

  > Kloak is a Keystroke Anonymization Tool.

- AudioContext Fingerprint - audiofingerprint.openwpm.com

  > This page tests browser-fingerprinting using the AudioContext and Canvas API. Using the AudioContext API to fingerprint does not collect sound played or recorded by your machine - an AudioContext fingerprint is a property of your machine’s audio stack itself.

- Available Fonts - orleika.github.io

  > Getting available fonts on browser without flash

- Browser Fingerprinting - niespodd.github.io
- BrowserLeaks - browserleaks.com

  > BrowserLeaks is all about browsing privacy and web browser fingerprinting. Here you will find a gallery of web technologies security testing tools that will show you what kind of personal identity data can be leaked, and how to protect yourself from this.

- Canvas Test - canvasblocker.kkapsner.de
- CSS Exfil Vulnerability Tester - mike-gualtieri.com

  > This page tests to see if your browser is vulnerable to Cascading Style Sheets (CSS) data leakage.

- Device Info - deviceinfo.me

  > Device Info is a web browser security testing, privacy testing, and troubleshooting tool.

- DNS Cookie Demonstration - dnscookie.com

  > DNS cookies use DNS caches as a side-channel to identify related network flows.

- EFF: Cover Your Tracks - coveryourtracks.eff.org

  > This is an EFF project that allows you to understand how easy it is to identify and track your browser based on how it appears to websites.

- Epic Tracker - epictracker.vercel.app

  > A demo of how can I track you using fingerprinting and some automated lookups and stuff, using modern Javascript APIs

- Extension Fingerprints - z0ccc.github.io

  > Chrome extensions can be detected by fetching their web accessible resources. These are files inside an extension that can be accessed by web pages. The detected extensions can be used to track you through browser fingerprinting.

  > This website scans over 1000 extensions and shows you the percentage of users that share the same extensions.

- Firefox Addon Detector - thehackerblog.com

  > Tracking 400+ Firefox Addons through chrome:// URI trickery!

- Iphey - iphey.com
- Mouse Wheel Tracking Test - jcarlosnorte.com
- Nothing Private - nothingprivate.ml

  > This project is a proof of concept that any website can identify and track you, even if you are using private browsing or incognito mode in your web browser. Many people think that they can hide their identity if they are using private browsing or incognito mode. This project will prove that they are wrong.

- PicassAuth - plaperdr.github.io

  > Canvas fingerprinting

- Pixelscan - pixelscan.net

  > Good, basically a bot check

- Privacy Check - privacycheck.sec.lrz.de

  > This website aims to focus on each fingerprinting technique in detail. It also presents the information and demonstrations in a way that is easy to understand, rather than giving a broad undescribed overview.

- scheme flooding - schemeflood.com

  > The vulnerability uses information about installed apps on your computer to assign you a permanent unique identifier even if you switch browsers, use incognito mode, or use a VPN.

- SuperCookie - demo.supercookie.me

  > Supercookie uses favicons to assign a unique identifier to website visitors.

  > Unlike traditional tracking methods, this ID can be stored almost persistently and cannot be easily cleared by the user.

> The tracking method works even in the browser’s incognito mode and is not cleared by flushing the cache, closing the browser or restarting the operating system, using a VPN or installing AdBlockers.

- Webgl Fingerprinting - webbrowsertools.com

  > This page uses different techniques to recognize whether a browser extension is installed to spoof the webgl fingerprint result or not. Sometimes to protect browser identity, a browser extension adds random noise to the canvas image (which is rendered in the GPU) and this noise alters the fingerprint result (hash code). Although the actual identity might be protected, there are still methods to detect whether the webgl result is manipulated or not. For instance, if manipulation is identified, the server may decide to ignore the webgl identity and uses a different approach to identify the browser session.

- Zardaxt.py - tcpip.incolumitas.com

  > TCP/IP Fingerprinting for VPN and Proxy Detection

- EOF

Sources & Kudos

- https://darknetlive.com/post/list-of-security-and-privacy-articles/
- https://darknetlive.com/post/list-of-fingerprinting-demo-sites/
- https://t.me/packet_pusher

Revision #4
Created 18 October 2022 01:12:57 by c0mmando
Updated 19 October 2022 17:16:24 by c0mmando