Keep your online life private!

ANONYMITY IN DIGITAL ERA

Every log file stored around the world will tell a story about you.

RICHARD WHITE

Anonymity in Digital Era

Every log file stored around the world will tell a story about you.

Richard White

This book is for sale at http://leanpub.com/anonymity_handbook

This version was published on 2014-03-29

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Tweet This Book!

Please help Richard White by spreading the word about this book on Twitter!

The suggested tweet for this book is:

just bought Anonymity Handbook

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

https://twitter.com/search?q=#

Also By Richard White

Privacy in Digital Era

Encryption in Everyday Life

Contents

Introduction

Today significant part of our communication takes place over the Internet, mainly through the services of different corporations.

Our digital lives are being recorded, it's the reality of the world we live in.

Every day, corporations & agencies around the world are recording lives of millions, they collect massive amounts of information about who we know, where we've been, and what we've done.

This surveillance apparatus can track the location of hundreds of millions of people, collect the phone records of the entire nation, and tap into the very backbone of the internet Is collecting millions of electronic records belonging to people who are not suspected of any wrongdoing.

The manner in which we use the internet influences our lives, data once written on the web stays on the web.

As a user, you need to be aware of risk, and the specific threats that are related to your methods of communication via Internet. Some of these risks are different, but as long as you're aware of them, you can manage them.

To become and remain anonymous online you need to use the Internet without giving anyone the ability to trace or link your web activity, or personal information, back to you.

What is Anonymity

> "A desire for privacy does not imply shameful secrets; Moglen argues, again and again, that without anonymity in discourse, free speech is impossible, and hence also democracy. The right to speak the truth to power does not shield the speaker from the consequences of doing so; only comparable power or anonymity can do that."
>
> —Nick Harkaway

Anonymous communications have an important role in our political and social discourse. Individuals desire to hide their identities because they may be concerned about political or economic retribution, harassment, or even threats to their lives.

Everything you do online leaves traces, and that information is considered very precious for commercial and intelligence purposes.

Majority of users are too quick to fill out forms or checkmark a yes box, or I agree box and to give out personal information on themselves online. Most of us don't see the internet as a threat until the un-imaginable happens.

As days go by it's harder to find online establishment that doesn't want some type of information about you. You even have your major store chains online asking for this stuff. So your information is being stored everywhere for everyone to see in one form or another. Even if the public online can't see this information, someone has access and is looking at it.

About the book

Anonymity Handbook is a practical, pragmatic guide with intent, to show you ways you can use to become and remain anonymous in digital realm.

Content of this book is important part of much broader area, presented in the book Privacy in Digital Era[1] which addresses the question of privacy in our society, and guides trough the process of achieving privacy by utilizing encryption methods, operating system hardening, data wiping and more.

You'll learn how to:

Encrypt your internet traffic.

Use anonymizing services (Tor and I2P)

Safely use your email.

Encrypt files in your Browser.

Properly use social networks and open web.

Most of all, this book will give you the power to control the information that you wish to reveal.

Book formats & versions available

The book is currently available in pdf, epub and mobi format, all included in the same price! The epub and mobi formats are best for reading on dedicated e-readers. Even if you are reading it on an e-reader, you may wish to download the PDF version as well for use on your computer.

Being published on leanpub.com, this book can easily be revised and updated. You will automatically be notified about any updates in the future.

Whichever versions you use, you will always get free access to all future updates to the e-book.

Author's website[2]

[1] https://leanpub.com/Privacy_in_Digital-Era

[2] http://digital-era.net

An important note for Windows and Mac users

Software solutions discussed run on Windows, Mac OS X, and Linux operating systems.

There is something else I want to bring your attention to!

To effectively use information provided in this book you should consider giving Linux a go. You need a reasonably secure system from which you can use Tor and reduce your risk of being tracked or compromised.

If for some reason you are unable to set up Linux, use Tails or Whonix (we covered Whonix in chapter titled "Encrypting your Internet traffic") instead, where most of this work is done for you. It's absolutely critical that outgoing access be firewalled so that third party applications cannot accidentally leak data about your location.

Few thoughts from Richard Stallman[3]

> Without Richard Matthew Stallman, who founded the Free Software Movement[4], there would be no GNU, and without GNU there would be no Linux distributions as we know them today.

People who use proprietary software [programs whose source code is hidden, and which are licensed under exclusive legal right of the copyright holder] are almost certainly using malware. The most widely used non-free programmes have malicious features – and I'm talking about specific, known malicious features.

There are three kinds: those that spy on the user, those that restrict the user, and back doors. Windows has all three. Microsoft can install software changes without asking permission.

When people don't know about this issue they choose based on immediate convenience and nothing else. And therefore they can be herded into giving up their freedom by a combination of convenient features, pressure from institutions and the network effect.

A proprietary programme gives you zero security from the owner of the programme. The users are totally defenceless and the owners often wipe the floor with the users because every non-free program gives the owner unjust powers.

People are aware that Windows has bad security but they are underestimating the problem because they are thinking about third parties. What about security against Microsoft? Every non-free program is a 'just trust me program'. 'Trust me, we're a big corporation. Big corporations would never mistreat anybody, would we?' Of course they would! They do all the time, that's what they are known for. So basically you mustn't trust a non free programme.

[3] http://en.wikipedia.org/wiki/Richard_Stallman

[4] http://www.fsf.org/about/

Conventions used in this Book

There's several conventions used through this book.

This is a Warning

You should really pay attention here, otherwise be prepared to deal with the consequences.

This is a Tip

Usually a piece or two of useful information.

This is an Information box

Special information here.

Terminology

I'll use some acronyms in this book. The first time I use an acronym, I'll write its expanded form in parenthesis, like this: AAG (Acronyms Are Great).

For your convenience, here's a short list of acronyms, abbreviations, and potentially confusing terms that I use in this book:

CLI Command-line interface. A textual interface for a tool that is meant to run in the terminal.

GUI A graphical user interface.

OS Operating System.

Anonymity

Every operation made in cyber space, every visited web site, and every web service accessed, leave traces of the user's experience on the Internet. This information is considered very precious for commercial and intelligence purposes. Private companies and governments are constantly monitoring the World Wide Web to collect and correlate the information to use in analysis on the user's behavior.

Surveillance and monitoring are activities of primary interest for many governments that in many cases trace political opponents with dramatic consequences that flow in fierce persecution. Recently the demand of anonymity has increased, mainly to respond to the large diffusion of surveillance platforms deployed all over the world, but the concept of anonymity induces fear in our imaginations due to the direct link that is usually made to illicit activities. It must be considered that anonymity on the web could also be motivated by noble argumentations, such as the fight for the human right to liberty of expression, avoidance of censorship, liberal promotion and the circulation of thought.

Anonymous communications have an important role in our political and social discourse. Individuals desire to hide their identities because they may be concerned about political or economic retribution, harassment, or even threats to their lives.

Surveillance apparatus exist, that can track the location of hundreds of millions of people, collect the phone records of entire nations, and tap into the very backbone of the internet.

Every day, the agencies records the lives of millions of Americans and countless foreigners, collecting massive amounts of information about who they know, where they've been, and what they've done. Its surveillance programs have been kept secret from the public they allegedly serve and protect.

Many internet users are aware of the risks when signing up to services provided by companies such as Google, Facebook, Twitter, and that Internet Service Providers (ISPs) have the ability to store data. Some may even know that cellphone carriers store all text (SMS) messages sent.

The awareness has been raised thanks to Wikileaks, the SOPA bill, firewalls in countries like China and now western countries (Australia and New Zealand have had firewalls for quite a while), and country-specific legislation which enables rights holders to request ISPs disconnect their customers with little proof of copyright infringement.

But when you talk with friends or family about this, quite often response is "I've got nothing to hide" or "I'm not special." Of course, you may not be special now, but who knows what might be considered "special" in the future?

It does not take much to accidentally stumble across something you should not on the web, log files are stored with ISPs and cloud services that don't have an expiry date. It is easy for governments to cherry pick information that is been collated through no fault of your own, and construct a story that fits their interest.

Every log file stored around the world will tell a story about you.

In the Internet, every machine is identified by its IP address that could be hidden by using anonymizing services and networks such as I2P and Tor network. Usually the anonymizing process is based on the concept of distribution of routing information. During the transmission of data between two entities in a network it is impossible to know the path between source and destination. Every node of the network manages minimal information to route the packets to the next hop without conserving history on the path. To avoid interception, encryption algorithms are used to make wiretapping impossible and to disable the recomposition of the original messages.

In this book we will cover:

Encrypting your Internet traffic.

Encrypting online communication.

Encrypting your email.

Online Habitats

Encrypting your Internet traffic.

Every operation made in cyber space, every visited web site, and every web service accessed, leave traces of the user's experience on the Internet. This information is considered very precious for commercial and intelligence purposes. Private companies and governments are constantly monitoring the World Wide Web to collect and correlate the information to use in analysis on the user's behavior.

Unsecured networks present a major threat to your security. You don't know who else is sharing the network, potentially intercepting and recording packets sent by your computer. Basic HTTPS web security does a good job of protecting data sent across the internet, but you are essentially at the mercy of the receiving site's security protocols. If you're transferring sensitive data, the sensible solution is to always use some kind of anonymizing service be it Tor, I2P or virtual private network.

```
1          Using Tor
2          Using I2P
3          Using encrypted VoIP platform
4          Using Whonix ( Anonymous Operating System)
5          Using VPN
```

Tor

Tor is a powerful, easy-to-use piece of software that lets you keep your online life private.

Tor provides truly anonymous and untraceable browsing and messaging, as well as access to the so-called "Deep Web" – a network of anonymous, untraceable, unblockable websites, available only through Tor, which provide everything from resources for political activists to pirated movies. The military-grade encryption behind Tor is so powerful that it can't plausibly be broken by any organization on the planet.

The web browser "Tor," part of the Tor Project, as it is called, was originally designed to protect Navy communications but is now being used by others for similar purposes. From the project's website:

Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others.

From the U.S. Navy Research Laboratory's Center for High Assurance Computer Systems:

The Onion Routing program is made up of projects researching, designing, building, and analyzing anonymous communications systems. The focus is on practical systems for low-latency Internet-based connections that resist traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routing servers themselves). Onion Routing prevents the transport medium from knowing who is communicating with whom — the network knows only that communication is taking place. In addition, the content of the communication is hidden from eavesdroppers up to the point where the traffic leaves the OR network.

How does it work?

Tor tunnels your traffic through an encrypted network of relays in which your IP-address can not be trace……