Health IT Security Journal

Volume 5, No. 1

A publication of the HITSF

HEALTH IT SECURITY JOURNAL

Volume 5, No. 1

A PUBLICATION OF THE HITSF

MAY, 2017

Letter from the editor

Dear readers,

This is the fifth year of the Journal and we are very proud to present another issue.

We at the Health Information Technology Security Forum are very excited about health information technology and how to secure it and ultimately, the patient data residing on those systems.

This issue of the Health IT Security Journal offers special features on privacy. We hope you can enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org.

Sincerely,

Hadi Syahrial
Editor in Chief

Techniques for maintaining anonymity and privacy on the Internet

Ramana Gaddamanugu

Have you ever wanted to watch a video and been stymied by a "this video is not available in your region" warning? Or maybe you've tried to leave an anonymous comment without a telltale IP address footprint? How about dropping a news agency an anonymous tip or blowing the whistle on wrongdoing? One of the ways around this problem is by using an anonymous Internet browser. One of the most popular types of this software is the Tor Project. This open source software, originally developed for the U.S. Navy, allows users to browse anonymously by using a global bank of Tor networks. Here we'll take a look at this and a few other anonymous browsing options that every geek should know.

Anonymous Browsing

Anonymous browsing works by encrypting traffic before it is sent out over the Internet. The IP address of the originating traffic and the destination IP are both encrypted inside the anonymous browsing packets. This prevents anyone from discovering the origin or ultimate destination of the traffic, preventing tracing of the user. The packets are encrypted, so if they happen to become misrouted, they still cannot be read. Once on the network, the packets are passed through a random series of servers on the anonymous browsing network until they reach the destination.

Although it may sound like a tool for hackers or software pirates, anonymous browsing has many uses. Businesses, for example, can use anonymous browsing to keep notes on competitors. Journalists and whistleblowers can also use this method to report news stories or dangerous behavior. Even regular Internet users who are concerned about their privacy can benefit from using an anonymous browser. (Read more about Internet privacy in What You Should Know About Your Privacy Online.)

ToR

One of the most popular anonymous browsing platforms is the Tor browser. Tor, short for The Onion Router, uses a worldwide network of anonymous servers to move traffic from location to location. Each packet passed through the network is wrapped in several layers of encryption. As the packet moves from server to server, a layer of encryption is removed. The wrapping of packets in several layers is akin to the skin on an onion, which is how Tor gets its name.

Tor is free to download and use and can be obtained from the Tor Project site, located at http://www.torproject.org. Tor comes in a number of different distributions and packages, but the easiest to download and use for anonymous browsing is known as the Tor Browser bundle. The package comes complete and ready to use. No installation is necessary. Once the package is downloaded, all that's required is to connect to the Internet and open the Tor browser. The Tor software handles all of the connections needed with no configuration by the user end. Within minutes you can be up and browsing anonymously.

Other Options

Although it is a popular solution, Tor isn't the only anonymous browser on the Internet. A number of different sites allow you to browse to different websites through use of their proxy servers. This solution is quick and easy and requires no additional software. Simply navigate to the website and type in the address that you wish to visit through the anonymous proxy. These websites are generally free services that allow you to keep your privacy when viewing pages on the Web, but they can be unreliable and may include advertising and pop-ups.

Paid Solutions

In addition to free solutions such as Tor and on-demand proxy browsers, software companies have rushed to fill the need for helping to protect privacy online. These solutions are typically solution-based, with the option to pay for your privacy by the month or by the year. Depending on the company, they may use hosted proxies, virtual private networks or a combination of methods to keep your information hidden from prying eyes. (Read more about VPNs in Virtual Private Network: The Branch Office Solution.)

Conclusion

What anonymous browsing solution you choose - or whether you choose one at all - will depend entirely on your browsing needs. First, you might want to start with the free and open source solutions to see if they address your privacy issues and concerns. If anonymous browsing is something that you want to do every day, or keep as a permanent solution, you'll probably want to investigate some of the paid platforms. These services will also have dedicated sales and tech support staff on hand to help address any issues or concerns you may have about anonymous browsing.

About the Author:

Ramana Gaddamanugu

Ramana Gaddamanugu is a privacy and fraud expert. He is a certified fraud examiner and a chartered accountant.

Privacy's New Normal: A paradigm shift for privacy

Eric Vanderburg

"See what we have here", the bearded vendor says as he displays an arm full of jeweled necklaces. "Rarities from around the world can be yours." As the customer looks at the beautiful gems, a street urchin lifts his wallet. "But alas," the vendor says, "you can hardly afford wonders such as these." I much the same way, technology has shown us wonderful things and while we imagined all the fantastic things we could do, someone – governments, companies, and others – was lifting our wallet; stealing our privacy.

The funny thing is that it seems normal. A colleague from a younger generation said to me one day, "Don't you know that privacy is dead?" I was taken aback at his frank assessment. The fact is that we have grown comfortable in our complacency.

In fact, generations from here on may well regard the lack of privacy as the "new normal" in which even cabs are ordered online; or conversations can be had with school systems through no mechanisms other than online systems; or routine shopping can be performed predominantly through online methods; or a Physician consult is through online mechanisms.

To such persons, this article may appear strange as to why the effects of loss of privacy are even be talked about. But, to others, there is time to pause and consider whether such a notion as privacy can even be assumed anymore; or we have reached a point of no return on the loss of privacy.

Only a tiny fraction of people change any behaviors in an effort to preserve their privacy. Few people turn down a discount at a restaurant or store by signing up for coupons or special offers. Go to any mall and you will find people giving away their information for a chance to win a prize. At the same time, consumers complain when organizations lose the same data they hand out every day.

As privacy threats multiply, defending this right to be left alone becomes more challenging. How do you know when you are left alone enough? How do you say when it's been taken? How do you measure what's lost? What is the real cost to a person whose Social Security number is in a data-storage device left in the back seat of a taxi?

So privacy does matter – at least sometimes. But it's like health: When you have it, you don't notice it. Only when it's gone do you wish you'd done more to protect it.

About the Author:

Eric Vanderburg
Vice President, Cybersecurity
TCDI

Eric Vanderburg is an information security executive, thought leader and author known for his insight on cybersecurity, privacy, data protection and storage. Some have called him the "Sheriff of the Internet" since he and his cybersecurity team at TCDI protect companies from cyber threats, investigate data breaches, and provide guidance on safe computing.

Eric is passionate about sharing knowledge of cybersecurity and technology news, insights and best practices. He regularly presents on security topics and maintains a security blog. You can find him throughout the day posting valuable content on his social media channels.

@evanderburg
inkedin.com/in/evanderburg
facebook.com/VanderburgE

HEALTH IT SECURITY JOURNAL

Volume 5, No. 1

HITSF

HITSF Journal

This journal is a publication of the Health Information Technology Security Forum, an international security organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and can be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health. Learn more at www.healthitsecurity.org

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.