Anonymity: Online Privacy Cum Security

Amit Dabas[1], Ashish Sharma[2]
[1,2]Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, INDIA

Abstract: **Anonymity is defined as a way of going through internet without any identity or hiding real identity of a user. The important idea here is that a person be non-identifiable, unreachable, or untraceable. Anonymity is seen as a technique, or a way of realizing, certain other values, such as privacy, or liberty. Anonymity is not direct solution but it's a method of using tools or network for privacy cum security. Low latency network like TOR are famous for this purpose and supporting the cause very well too. In this research being anonymous is not the only aim but to provide security and anonymity under the radar of Law & Jurisdiction.**[1]

Keywords— Anonymous, TOR, Online Privacy, Anonymity

I. INRODUCTION

An important example for anonymity being not only protected, but enforced by law is probably the vote in free elections. In many other situations (like conversation between strangers, buying some product or service in a shop), anonymity is traditionally accepted as natural. There are also various situations in which a person might choose to withhold their identity. Acts of charity have been performed anonymously when benefactors do not wish to be acknowledged. A person who feels threatened might attempt to mitigate that threat through anonymity. A witness to a crime might seek to avoid retribution, for example, by anonymously calling a crime tipline. Criminals might proceed anonymously to conceal their participation in a crime. Anonymity may also be created unintentionally, through the loss of identifying information due to the passage of time or a destructive event.

In certain situations, however, it may be illegal to remain anonymous. In the United States, 24 states have "stop and identify" statutes that requires persons detained to self-identify when requested by a law enforcement officer. In German, people have to indicate their names at the door of their homes[1].

II. WHO NEED ANONYMITY?

As consumers increasingly go online in so many aspects of their daily lives, the challenge is enjoy the conveniences of online activities while limiting the privacy sacrifices. As the focus of online activity migrates from desktop and laptop computers to smartphones and other mobile devices, the mechanisms for protecting their privacy continue to evolve.[(online-privacy-using-internet-safely, n.d.)]

Most internet users would like to be anonymous online, but many think it is not possible to be completely anonymous online. Many internet users have experienced problems because others stole their personal information or otherwise took advantage of their visibility online.

Anonymity helps military research work, private online users in their privacy, blocked users to reach to the information online, corporate organizations to be secure and safe on internet.

III. PRIVACY ATTACK FACTORS

As all online users need to give and take information on internet by some mean so there are many ways there security or privacy get compromised sometimes by users lack of knowledge sometimes tricks used by hackers or data collectors .

Methods of Information Leakage by user
• Signing up for Internet service
• Browsing the Internet
• Search Engines
• Cookies
• Flash cookies
• Fingerprinting
• Householding
• Using Mobile Apps
• Using e-mail
• Instant messaging
• Social networking
• Maintaining a personal website
• Blogging

Table 1: Methods of information leakage by user

As in the above table are the daily or most common activities performed by users and they lose their data which could be compromised somehow by collecting more information of a user but there are then way where user gets tricked or hacked to loose important data to hackers or data collectors. Those are more defined data attacks as what data the marketing needs is collected.[2]

Methods of Information theft
• Marketing
• Web bugs
• Direct marketing
• Behavioral marketing or targeting
• Location tracking
• Employee monitoring
• Government surveillance
• Court records
• Shopping online
• Illegal activity and scams
• Malicious links

Table 2: Methods of information theft

IV. BASIC TOOLS FOR ANONYMITY

Following is list of basic Anonymity tools which could be run and used by basic internet user for privacy cum security.

- **Tails**: live operating system that can run from removable media without leaving tracks. Routes Internet traffic through the Tor network.
- **Tor** (Windows, OSX, GNU/Linux, BSD, Unix): Internet anonymizing software that securely routes traffic through multiple nodes around the world. Open source, free.
- **Orbot** (Android): Tor client for Android.
- **Anonymizer**(Windows, OSX, Linux, iPhone, iPad, Android): Encrypts and anonymizes Internet traffic.
- **CyberGhostVPN** : Easy to use VPN service.
- **IPreadator**
- **I2P Anonymous Network**
- **Private Internet Access**
- **proXPN**
- **StrongVPN**
- **torVPN**
- **TorGuard**
- **VyprVPN**
- **WiTopia**
- **Proxy.org:** lists thousands of proxy sites.
- **Proxify**
- **TunnelBear** (Windows, OSX, Android, iOS)

Web Browser Ad-ons

- **HTTPS Everywhere** (Firefox, Chrome): forces HTTPS versions of websites were they are available.
- **Adblock Plus** (Firefox, Chome, Opera, Android): customizable ad-blocking plugin
- **NoScript** (Firefox, derivatives of Mozilla): highly customizable plugin to selectively allow Javascript, Java, and Flash to run.
- **Disconect** (Firefox, Chrome, Safari, Opera): stops 3rd party tracking sites around the web.
- **BetterPrivacy** (Firefox): removes and deletes long-term “super-cookies”

Search Engines

- **DuckDuckGo**: anonymous, encrypted web searches.
- **ixquick**: anonymous, encrypted web searches. Hosted in the Netherlands.

Email/Communication Encryption

- **GPG**(Windows, OSX, Linux): free implementation of OpenPGP.
- **Mailvelope**(Chrome, Firefox): OpenPGP encryption for webmail.
- **Enigmail** is and OpenPGP add-on for the Thunderbird and SeaMonkey email clients.
- **GPGMail** is a plug in for Apple Mail, an open source implementation of OpenPGP for encrypting, decrypting, signing and verifying email.
- **Email Self Defense**: a guide for using encrypted email (GNU/Linux, Mac OS, Windows).

Alternative Email Accounts

- **Guerrillamail**: web-based disposable email accounts.
- **Tor Mail**: anonymous email provider (Tor required).
- CounterMail
- **MyKolab**: Privacy-focused email, based in Switzerland
- **Neomailbox**: email provider focused on privacy and anonymity, based in Switzerland[5]

V. TOR: ANONYMIZER NETWORK

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information [2]over public networks without compromising their privacy.

Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.[3]

Journalists use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization.

Groups such as Indymedia recommend Tor for safeguarding their members' online privacy and security. Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online. Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers. They also use it to replace traditional VPNs, which reveal the exact amount and timing of communication. Which locations have employees working late? Which locations have employees consulting job-hunting websites? Which research divisions are communicating with the company's patent lawyers?[6]

VI. TOR ROUTING ALGORITHM & ENCRYPTION METHOD

Toris a distributed system containing a handful of authorities that assist in distributing a consensus of trusted relay information. This directory of relays informs clients about the stability of and resources provided by each relay.[4] Clients use this information to select relays for their circuits: the choice is weighted by the relative difference in the perceived throughput of each relay in an attempt to balance network load. Although Tor's main purpose is to protect a client's communication privacy, it also serves as a tool to resist censorship[(Perry, 2007)].

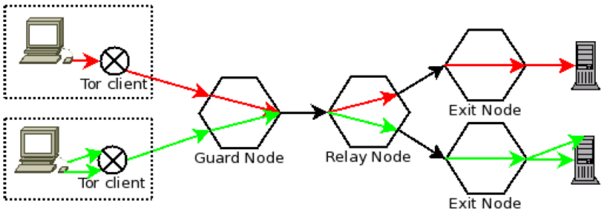

Fig 1: Information provided to the clients

VII. CONCLUSION

Online anonymity is important and need of online users with growing amount of cyber-attacks like identity thefts snooping of networks. So important that Canada's Supreme Court recently declared it vital to personal privacy in the digital era. But plenty of countries disagree, including the Internet's greatest enemies and even some alleged "friends." Brazil, home to the celebrated "Internet Bill of Rights," still prohibits anonymous free speech. Such prohibitions usually come down to political control under the guise of national security[7].

Despite new mediums and platforms, "who to trust" is not a new question. The same logic that once applied when reading about Bat Boy in the tabloids still applies online.

Be skeptical. Be incredulous. Be diligent. Ask questions. Seek information from multiple sources. In essence, pretend you're a journalist.

Just because you can't distinguish fact from fiction or occasionally get burned by abusive trolls doesn't mean we should write off the enormous benefits online anonymity can bring to people who need it most. Need of Anonymous network under control of governance could be boon for e-governance and its users too[8]. Freed speech journalists can use it as a safety point.

REFERENCES

[1] *Anonymity*. (n.d.). Retrieved from http://en.wikipedia.org/wiki. *about/overview*. (n.d.). Retrieved from www.torproject.org.

[2] Danezis, S. J. (n.d.). Low-Cost Traffic Analysis of Tor.

[3] Ekstrand, V. S. (2010). Unmasking Jane and John Doe: Online Anonymity and the First Amendment. 405-427.

[4] *online-privacy-using-internet-safely*. (n.d.). Retrieved from www.privacyrights.org.

[5] https://epic.org/privacy

[6] Reed, M. S. (1998). Anonymous connections and onion routing. *Selected Areas in Communications, IEEE Journal* , 482 - 494.

[7] Simone Quatrini, M. R. (2011, June 13). *http://www.ihteam.net/papers_tutorial/*.Retrieved 6 25, 2014, from http://www.ihteam.net: http://www.ihteam.net//papers/blind-sqli-regexp-attack.pdf

[8] *why-do-we-need-privacy-anyway*. (n.d.). Retrieved from www.privateinternetaccess.com.