Security and Privacy

Saurabh Mahendra Jadhav
Atharva College of Engineering (CMPN)
Mumbai,India

Abstract:- **The entire computer security field is based on three cornerstones those are Confidentiality, Authenticity, Availability and if one of these principles are violated then security and safety of an individual & collective is compromised. The problem with technology is that when we introduce new type of technology it creates vulnerabilities for the existing once and as hacking crimes and carefully planned computer attacks are being executed, Anonymity is the key to an individual's privacy as well as to a group. Keeping personal information and online activities unprotected is not a good idea. In this study it is demonstrated how to protect anonymity and the importance of protecting anonymity to prevent any exploitation to the safety and privacy of individual as well as collective.**

Keywords:- Dark Net; Deep Web;Tor Services; Ethereum; MadeSafe; Safe Communication.

1. INTRODUCTION:

Security privacy and safety are very crucial and important part of an individual's online activity and little bit of carelessness can cause a lot of damage, privacy on internet is counter intuitive because every move of everyone is being recorded and internet never forgets anything in such case "Anonymity" is the only way forward. Importance of security privacy and safety in communication, work and online activity is unmatched, to achieve anonymity in these areas "Dark Net" and "Deep Web" can be used. The biggest problem with the internet is that there is no anonymity in the web and even the use of most advance password creation techniques and high measures of security, it is possible to break in with enough work with free operating systems like Kali linux which contains more than 900 hacking tools or in academic and legal term known as penetration testing tools and other big advantage of Kali is a linux distribution and it is open source this allows the million of activist and technology geeks to work on it and use it as they want this results in staggering amount in innovation as well as it gives unpredictability and vulnerability

In 2004 The sony company was hacked by north Korea which was later confirmed by president Barack Obama that hacking attack proved that even with very high security measures it is possible to do mass destruction. Since the revolution started by Edward Snowden it is clear that anonymity is the most important thing Edward Snowden pointed out how the government agencies like CIA, NSA have the most advanced surveillance capabilities, it is not just these agencies are using them but it is practiced all around the world by almost all governments of all countries around the world to prevent terrorist attacks but same techniques are being used by the blackhat hackers for the wrong purpose.

2. LITERATURE SURVEY

The dark net and deep web are basically distributed computing applications, At fundamental level dark net and deep web are distributed computing but with powerful encryption, which makes everything very hard to censor and monitor.

The visible results from search engines like "google","duck duck go" or "Bing" is known as the visible internet. Dark net is anything which is not visible in these search engines in other words anything which is not indexed on these search engines is known as dark net. Dark net is network and deep web are similar terminologies as dark net but related to websites.Dark net and Deep web tools are designed for staying highly anonymous and everything is cleverly encrypted, At fundamental level dark net and deep web are distributed computing but with powerful encryption, which is very hard to censor and monitor.

2.1 The Dark Net

Dark net is a net work of computers which is not accessible or reachable from google or other search engines eg. college lab networks, office networks. which the google or any other search engine needs not to know or simply they don't care, Any network which is not indexed or which is not accessible from browsers like chrome or firefox is considered as dark net

2.2 Deep Web

The collection and inter connection websites which are not accessible from normal browsers like chrome or firefox means which are not indexed on any search engine known as deep web.

Deep web sites are not like normal websites and no one can access these sites without a browser called tor browser, deep web sites does not have URL like normal websites they are meaningless numbers, strings and characters which ends up in ".onion" and called as onion address

2.3 Tor

Tor was originally the US naval intelligence's side project it was built for undercover officers to communicate with officials from difficult places afterwards it became open source and now it allows anybody to browse he internet without giving away their location, Preventing the monitoring is managed by encryption the IP address and it is sent to another node around the world in different country and there it is decrypted and this process is done several times so when ultimately the request reaches to the internet from dark net it is practically not traceable where it came from but the user of the service can manage to use the privileges as like normal browsing Tor is not the only solution for anonymity, It needs to be coupled with other privacy enhancing tools for absolute

anonymity but even without privacy enhancing tools it is very hard to perform surveillance or eavesdrop on anyone . Tor is an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content. Journalists use Tor to communicate more safely with whistleblowers and dissidents. A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East recently. Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations. The variety of people who use Tor is actually part of what makes it so secure. Tor hides you among the other users on the network, so the more populous and diverse the user base for Tor is, the more your anonymity will be protected.

2.3.1 Orbot

Android is a platform managed by developed by google and google says that there are more than 1.4 billion android active devices yet many people use older version of the operating system which compromises the system's security. A new update fixes the problem so if consumer is running on older version then the vulnerabilities in their device is not removed, nowadays people keep a lot of sensitive information on mobile devices. A vulnerable device with a lot of sensitive data is always best target for any attacker to carry out eavesdropping to steal valuable information Orbot is a free proxy app that empowers other apps to use the internet more securely. Orbot uses Tor to encrypt your Internet traffic and then hides it by bouncing through a series of computers around the world Orbot creates a truly private mobile internet connection.

2.3.2 Tor Messenger

An extremely common way and easiest way to communicate is texting and if that communication is not secure then there is chance of sniffing attack to monitor and collect valuable information by attackers Tor Messenger is a cross-platform chat program that aims to be secure by default and sends all of its traffic over Tor. It supports a wide variety of transport networks, including Jabber (XMPP), IRC, Google Talk, Facebook Chat,Twitter, Yahoo. Tor Messenger builds on the networks you are familiar with. This has traditionally been in a client-server model, meaning that your metadata can be logged by the server. However, your route to the server will be hidden because you are communicating over Tor.

2.4 Why We Need Tor

We live in a world which is changing at an exponential rate and sometimes issues arise around the world which causes violation of human rights and conservation of them can be very tricky, to be able to speak makes and allow your voice for people to listen is great asset and with normal internet it is not always possible Tor browser gives us high degree of anonymity and create a distributed network that no one really controls. It is censorship free anonymous world visited by anonymous people .The online education allows everybody to learn everything they want wherever they want it does helps to improve the society but it also allows anybody to be able to hack and mine valuable sensitive information which was previously not available, having knowledge about everything is always good for innovation but it also compromises the privacy of million of people around the globe, hacking courses online teach from beginner to advance hacking techniques in such case privacy maintenance is necessary and tor protects the privacy online.

3. ETHEREUM

Ethereum is an open blockchain platform that lets anyone build and use decentralised applications that run on blockchain technology. Ethereum is an open-source project built by communities around the world related to their interests. Ethereum was designed to be adaptable and flexible. It is very convenient to create and build new applications. Ethereum incorporates many features and technologies that will be familiar to users of Bitcoin, while also introducing many modifications and innovations of its own. Ethereum's basic unit is the account. The Ethereum blockchain tracks the state of every account, and all state transitions on the Ethereum blockchain are transfers of value and information between accounts. There are two types of accounts: Externally Owned Accounts (EOAs), which are controlled by private keys Contract Accounts, which are controlled by their contract code and can only be "activated" by an EOA. Contract accounts, on the other hand, are governed by their internal code. If they are "controlled" by a human user, because it is they are programmed to be controlled by an EOA with a certain address, which is in turn controlled by whoever holds the private keys that control that EOA. The popular term "smart contracts" refers to code in a Contract Account – programs that execute when a transaction is sent to that account. Users can create new contracts by deploying code to the blockchain.open source nature of ethereum is shaping the internet ethereum is not only valuable for heavy softwares but also for IoT's which brings more flexibility to ethereum. A real life example of innovation in the field of IoT is slock.it . slock.it is a application of blockchain platform which allows the users to buy sell or rent things, slock.it can be embedded in any smart device easily. slock.it is a physical smart lock which allows the users to use the service by paying for it over block chain platform and decentralised nature of blockchain and slock.it makes it very hard to hack.

4. MAIDSAFE

A huge amount of sensitive data is uploaded on cloud every day and readily availableness it is an easy target for hackers also cloud companies have to work under the law and if they require then cloud companies have to disclose their data to governments but cloud is so much easy to use and very useful platform yet it is not distributed that makes it vulnerable.A block chain type project called Maid safe allows users to store the data on cloud in a decentralised manner. Files uploaded to the network are broken into pieces, encrypted and distributed across the network. This process is called Self-Encryption. This process ensures that only the owner of the data and not anyone else is able to modify or remove it.

The network is programmed to keep duplicate copies of each piece of data at all times. As users turn their computers off, the network makes more copies and stores. Them on other machines, ensuring that users always have access to their files.

This constant movement of data (called churn) is a key part of the security that the SAFE Network offers because there is no central point for hackers to target as the data locations keep changing.

5. PROTON MAIL

Proton mail is an end to end encryption for secure communication and it is free of cost but professional features are only for paid users. Messages are stored on ProtonMail servers in encrypted format. They are also transmitted in encrypted format between our servers and user devices. Messages between ProtonMail users are also transmitted in encrypted form within our secure server network. Because data is encrypted at all steps, the risk of message interception is largely eliminated. Proton mail work on principle of zero access to user data it means only sender and receiver are able to access the data. proton mail keeps all the values of computer security unviolated which are Confidentiality, Availability and Authenticity that makes proton mail very reliable as compared to gmail where beginner's hacking courses have hacking techniques in syllabus even.

6. APPLICATIONS

- prevention of location tracking by IP (internet protocol)
- Encrypted browsing
- Safe online Storage
- Research in Sensitive topics Anonymously
- Curation of human rights around the globe by Ability to report anonymously
- Safe Project management
- prevention of being a victim of mass surveillance

7. CONCLUSION

An individual's security and online does matters, and there are millions of activists around the world who are working on tool and techniques to keep people private and safe online but Safety and privacy is a real case of mind over matter if you don't mind then it doesn't matter. Since the revolution from Edward Snowden there has been huge increase in the people using privacy enhancing tools and now around daily about a more than 10 million people are using tor browser daily and the use of tor browser is perfectly legitimate.

REFERENCES:

[1] Jamie Bartlett: "the dark net".
[2] http://www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system
[3] http://www.ted.com/talks/jamie_bartlett_how_the_mysterious_dark_net_is_going_mainstream
[4] https://www.youtube.com/watch?v =d7pjA7vFds4&t=63s
[5] https://protonmail.com/security-detail
[6] https://developer.android.com/about/dashboards/index.html
[7] http://www.androidcentral.com/google- says-there-are-now-14-billion-active-android- devices-worldwide
[8] https://www.udemy.com/courses/search/?q=hacking&src=sac&kw=hack&lang=en
[9] https://slock.it/index.html
[10] http://www.kalilinuxdojo.com/2016/09/brute-force-attack-to-hack-gmail-password-using-hydra-and-kali-linux.html