***Onion networks and onion routing***

***Author:***

***IBXXXX***

***Faculty of Information Technologies Mostar***

***University:University of Dzemal Bijedic Mostar***

***1.Introductory:***

We live in the world where our lives have become dependent of the technologies we use every day. Some experts say that this will affect us in the long run and that in 50 or more years from now we will be merged with the technology completely. Internet, when it first came to be, was a breakthrough. Who could have thought that the internet would be used in amounts it is used today. Many people use it and still don’t know how It works. Many also compared it with magic when it first came to be. Truth is that, behind the thing called the internet lay foundations of many other technologies, rules of physics, mathematical algorithms and protocols that now, a simple internet user, would need a lifetime to fully understand the inner workings of this magical thing he uses every day, sometimes without even knowing it. With internet came also many dangers that some people who were more skilled and knew kore than other user could use this against them. This is why privacy was a major concern when it came to designing and implementing the whole internet. Anyone could become anyone, and this presented a problem. Many countries around the world also had strict policies regarding what their citizens and users of the internet could see, watch or interact with. This lead to the development of some technologies we will be talking about in this research. Term anonymity on the internet soon became a thing and today it completely changed the way we look at the this magical communication technology.

***2. Brief history of the onion routing:***

In the 1990s, the lack of security on the internet and its ability to be used for tracking and surveillance was

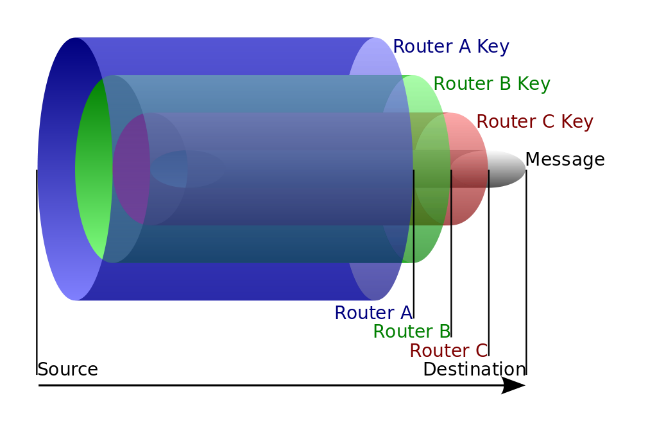
becoming clear [1] .In 1995, *David Goldschlag,* *Mike Reed*, and *Paul Syverson* of the U.S. Naval Research Lab wanted to create internet connections that don't reveal who is talking to whom, even to someone monitoring the network. It was further developed by the Defense Advanced Research Projects Agency and patented by the Navy in 1998. This would allow the internet users to become fully anonymous and would solve the above mentioned problem. This is when the idea and a concept of onion routing was created . The goal of onion routing was to have a way create as much privacy as possible, and one of the ideas was to make the traffic go from one computer on the overlay network to another, thus creating a route which was untraceable. It was called onion routing because of this. Encryption of the traffic would in theory be applied on every node the traffic goes to. From its inception in the 1990-s, onion routing was designed to be a decentralized network. The network needed to be operated by entities with diverse interests and trust assumptions, and the software needed to be free and open to maximize transparenc. In 1998, there were multiple independently deployed networks of around many nodes each running on multiple platforms ( mostly Unix based, Solaris, Linux, Windows NT, BSD), but none of these designs was ever publicly accessible. In the early 2000s, *Roger Dingledine*, a MIT graduate, began working on an onion routing project with *Paul Syverson*. Soon other onion routing implementation were popping everywhere and Roger and Paul wanted to name their project. It was called TOR which stood for The Onion Routing [1]. This is probably the most used and most well known type of onion routing nowadays. Tor became an open source projectin 2006 and soon was accepted by the community from all around the world [2].



*Picture 1. The Onion Routing project*

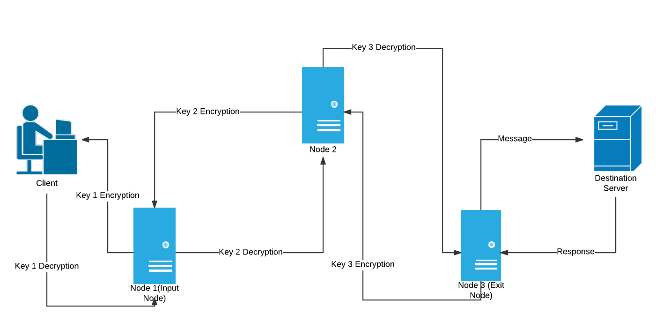
***3. Onion routing circuit*:**

Onion routing is basically a technique used for anonymous communication over internet by creating an overlay network we call an onion network. Similar to a real onion it enforces encryption on each node the traffic passes and by achieving this it creates layers of encryption, so if someone sniffs on one node it can’t see the traffic because it is encrypted by a key of the previous node. If you for example, want to send an HTTPs request to a server and someone intercepts that request it would still be able to know which server you are contacting. This is where onion routing kicks in , by bouncing your request from one server to another and then forwarding it to the intended server. Anyone sniffing would only see the traffic destined to a node which my be or may not be the server node the user requested [3].



*Picture 2. Onion routing encryption example, layers of an “onion”*

Using normal browsers like firefox or chrome we make simple GET requests when requesting pages from the server. It is a two way communication where the client opens connection to the server and transmits information with it. As mentioned before, anyone sniffing could see the destination server. In onion routing the servers, or nodes, as they a re called all maintain the connection between each other, so when the client requests the content of the web page it goes back from the destination server using the same route it took to the destination server from the user node [3]. Each router encrypts the message when it passes, so every node has only one key, but the client initiating the connection has all the keys used for decryption. This is very similar to a VPN where we use another server to get our requests for us, but in this example we can have many servers. This makes the process a lot slower so using onion routing for downloading, streaming or performing any heavy usage of the network is not preferred.



*Picture 3. Onion routing simplified using 3 nodes*

When talking about the nodes, everyone on the internet can become a node on the Tor network by simply installing the software needed. A user can be both a user and a server node if he wants to.

***4. Onion routing encryption*:**

Onion encryption is based on socket connections that are resistant to both eavesdropping or sniffing and traffic analysis. The confidentiality of these socket connections has been transferred below the application level and made independent of the applications. Standard Internet applications can use these anonymous connections by using onion proxy servers which are part of the onion network. The application, instead of opening a connection directly to the destination machine, opens connections to the onion proxy server. This proxy server creates an anonymous connection through a set of other onion routers to the destination [4]. Every onion router in the path maintains an routing table of all his neighbors just like in normal communication. Before it sends the data it received over an anonymous connection it first adds level of encryption for each router the data will travel to. In the process of transferring data over an anonymous connection, each router removes one level of encryption, thus, the data eventually arrive in plain text. When moving data in the opposite direction, this layering of encryption occurs in the reverse order. It is worth noting that after the connection is broken, all information about this connection is deleted on all onion routers. In the above example where we used 3 nodes to communicate to a server we will say we exchanged three symmetric keys between the three nodes on the network using Diffie-helmans exchange. So basically the client which has all the 3 symmetric keys uses DH exchange to acquire the public keys from the servers. Then the client encrypts the data with his 3 keys and sends it to the router which contains the symmetric key used to encrypt it the last time, so this node will only be able to encrypt the “outer” layer. This node then forwards it to the next and the data gets to the destination server in plain text. On the way back each router in the network adds encryption (AES in counter mode with a key length of 128 bits) with it’s key which finally ends on the client side 3 times encrypted, but the client has all the 3 keys because he is the one who generated them. The only thing the nodes know is that they need to add or remove a layer of encryption and then forward it to the next router in the routing table. This prevents them from knowing who the client is , and what is he requesting. Input node or the first node knows only that the client is using tor, and the final node( exit node ) only knows that it is communicating with the destination server [5]. So simply, directory server periodically uploads the list of nodes that are available for relaying data. Each node is publicly known and some ISP’s, in some countries block every request to these nodes, preventing the users from using the onion routing. This can be circumvented by using bridges which we will cover later. Client selects three nodes from this list and gets their public key using which it encrypt data multiple times and sends data to first node of the circuit. Each node in the circuit decrypts one layer using their private key. and exit node send data to the destination. Bridges, or bridge relays are simply tor nodes that are not publicly listed. That means that ISPs or governments trying to block access to the Tor network can't simply block all bridges[5].Anyone using the tor network can be a bridge and help the community in which more oppressive regimes are employed. Several countries, including China and Iran ISPs have forbid acces to many tor bridges but this can also be avoided by using Obfsproxy bridges which add an additional layer of obfuscation.

Slika koja sadrži tekst

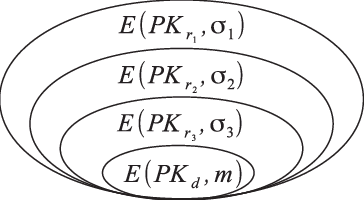
Opis je automatski generiran

*Picture 4. Node circuits*

*Slika koja sadrži tekst

Opis je automatski generiran*

*Picture 5. Tor bridges configuration*



*Picture 6. Encryption keys on the onion network*

***5.The Onion Router (TOR)*:**

Probably the most known service when it comes to using the onion routing protocol is the Tor project. Tor began gaining popularity among activists and internet users interested in privacy and anonymity, but it was still difficult for less-tech savy people to use, so in 2005, development of tools beyond just the Tor proxy began. Development of Tor Browser began in 2008. Tor browser is a software which is easily installed on both windows and linux machines that provides access to the onion network. Besides tor browser there are other similar tools. Many people also use the tor service in conjuction with the proxychains tool In order to proxy their traffic through tor. This is also used by criminals when conducting hacking activites. It found it’s use in many countries where censorship is strict. Many journalists use it and it is basically a standard when it comes to onion routing. It is based on the open source Mozilla Firefox browser but it adds more options regarding your privacy and allowing users to use the TOR overlay network when surfing the web.

Slika koja sadrži tekst

Opis je automatski generiran

*Picture 7. Tor browser front page*

Tor is a distributed overlay network used to anonymize applications using low latency TCP connections. Users use onion proxies to access the Tor network. Onion routers establish TLS connections between other routers, and the onion proxies connect by establishing a TLS connection with one or more onion routers. The purpose of this network is to prevent third parties or participating nodes from associating the sender of the message with the recipient. Clients send the data using the fixed circuits inside TOR. These circuits can be changed accordingly. A circuit consists of three nodes by default, just like the before mentioned example, but it can consists of many more nodes.

In the Tor network, all data exchanged between nodes is encapsulated into cells. In most cases, the cells have a fixed size. In version 4 and above, the fixed cell size is 514 bytes, and each cell consists of a header and a payload. The header consists of a chain identifier CircID field which is used by the nodes to know to which next node to send the data to. It is 4 bytes in size. The last is the command, which indicates what needs to be done with the payload of the cell [5].

Slika koja sadrži tabela

Opis je automatski generiran

*Picture 8. Tor data cell*

***6. TOR implementations:***

Although we can say that we are in the most part safe and our privacy is untouched when using the TOR browser other components of our network architecture and our operating system can cause information leakage and increase our chances of being noticed and disrupting our anonymity using the onion routing. This is the reason why the open source community developed Operating systems used specifically in combination with the TOR to offer its users nearly maximum level of security, privacy and anonymity. One of them is Tails OS. It is a Live operating system that utilizes onion routing to route all the traffic coming from the system through the tor network. It is live which means it stores everything inside the RAM memory and when it is switched off you start from scratch. This helps in hiding your network fingerprint and discovering things you did on the system like browser history and such things. One better system is definitely is Whonix which is also a Debian based distribution which uses virtual machine deployment for each task you need it to perform. For example one VM is used for browsing the internet and the other for storage. Tor also started implementing the Tor messenger which allowed message communication through the onion routing protocol but they gave up on this project and is currently deprecated[6].



*Picture 9. Tor messenger*

**

*Picture 10. Tails OS*

*OnionShare* is a sharing system used with TOR for exchanging files anonymously. It comes installed by default on TailOS [6].

The Guardian project, global collective of software developers, designers, activists also plans to implement TOR inside Android mobile phones. Some mobile applications they developed include *ORBOT* which is a proxy, *ORFOX* that acts like a Tor browser and *ChatSecure*, similar to Tor messenger.

Tor has been praised for providing privacy and anonymity to vulnerable Internet users such as political activists fearing surveillance and arrest, ordinary web users seeking to circumvent censorship, and people who have been threatened with violence or abuse by stalkers. It is unfortunately used also by criminals and terrorist organizations, of which we will see later.

***7. The Dark and the Deep web:***

There is a lot of misconceptions about the definition of the dark web and the deep web. Deep web simply refers to those pages on the internet( both clear internet and the internet we access using the onion router ) that haven’t been indexed by search engines like Google, Bing, Baidu .Those include administration panels, user panels, forums and mostly sites protected by authentication. Dark web on the other hand is something that exists only and can be accessed only by using onion routing or using the before mentioned TOR browser [7]. People often use the analogy of the iceberg when talking about these two. Normal browsers like google chrome can’t access sites on the dark web which have the extension .onion instead of the normal top-level domain we are used to when browsing the “normal” internet.

Slika koja sadrži karta

Opis je automatski generiran

*Picture 11.. Iceberg analogy*

.onion addresses are not dns names , but internet programs such as TOR browser can access sites with .onion addresses by sending the request through the Tor network. This is mainly implemented to provide the client and the server providing the information more anonymous and untraceable. These sites can also implement HTTPs communication using TLS encryption which adds another layer of security, since most of the onion sites are using http only nowadays. Addresses in the .onion TLD are randomly generated between 16 and 56 characters both alpha and numerical strings which are generated based on a public key when the server configures the onion service. It is possible to make the URL look more human readable like in Picture 12. but this requires a large number of public key generations in order to achieve this [8].

Slika koja sadrži tekst

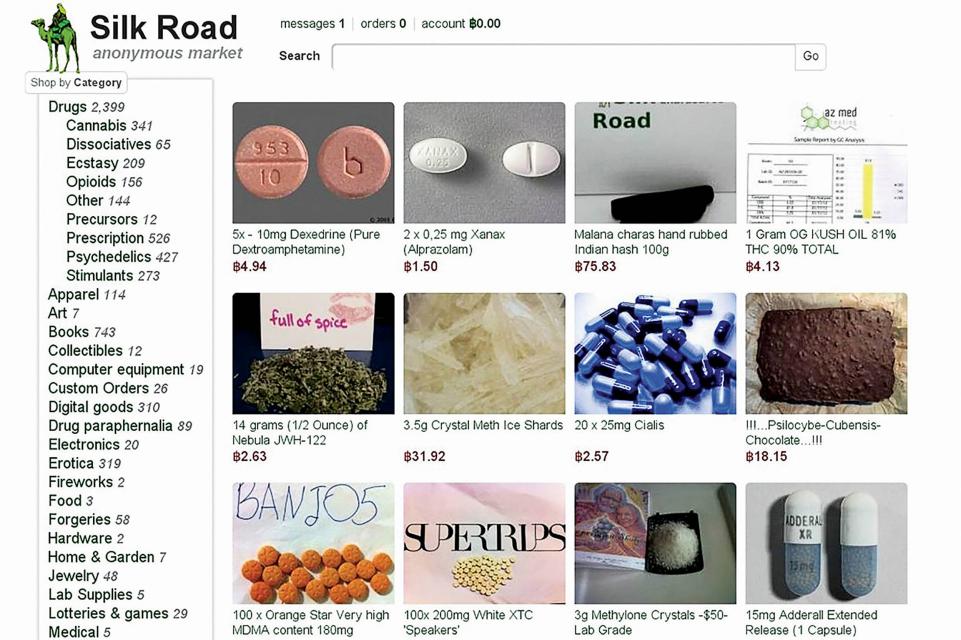
Opis je automatski generiran

*Picture 12.* [*http://avengersdutyk3xf.onion/*](http://avengersdutyk3xf.onion/) *address*

Proxies like Tor2Web can also be used in order to allow normal web browsers to access tor hidden services ending with .onion. Many famous websites like Facebook, Google and other have .onion counterparts, and are used by people in countries where social network like these are forbidden(North Korea for example).

* ***Hidden Services:***

Hidden services are just websites ending with .onion address accessed only through onion routing that provide users with some services. As soon as the dark web was implemented many online markets started appearing. Online markets where nothing new but in combination with the tor network it allowed the buyer and the seller to remain anonymous. Drug markets are the most popular markets that one can find on the dark web but many others which sell weapons, passports or even children pornography exist. Like all innovative tools, the dark web is used also for shady and illegal activities.[9] One of the most popular online dark web markets which was eventually seized by the FBI is *the Silk Road.* The owner of this hidden service is now serving a life prison sentence.



*Picture 13. Silk road Drug market*

**

*Picture 14. Isis terrorist group webpage*

The day after the FBI shut down the market a new one called Silk Road 2 appeared which shows that this trend is not going to stop.

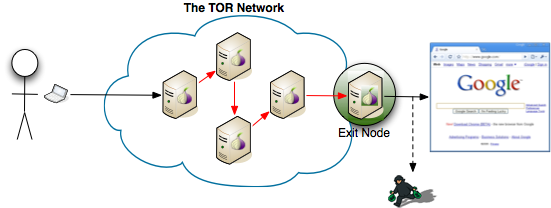
Another example is the famous whistleblower Edward Snowden who used tor hidden services to deliver confidential documents regarding the American National Security Agency. In countries where the government restricts access to specific websites and social media networks dark web tools can help circumvent censorship[10].

***8. Onion routing security:***

Tor is an interesting and well-designed system, but like any computer system, it has vulnerabilities. This is something that every tor user should consider when using it. You might think that everything you do is 100% secure, but if you think about it from the attacker’s perspective you will see some holes. The attack that took place a couple of years ago shows this. Just by controlling a great amount of tor nodes attackers were able to sniff the network and figure out where to and from the packets where going. This has become a trend since then, because Tor is an open source project and everyone is free to contribute, including the attackers. So basically if the attackers controlled both the entry node and the exit node they would be able to see the traffic and deanonymize the part of the overlay network. Also when talking about encryption tor doesn’t support end-to-end encryption so when the data exits the exit node it is in plain text. This is true for most of the websites that don’t use HTTPs. One Swedish researcher used such an attack to collect the passwords of over 100 emails, but this could have easily been done by an attacker.[12].

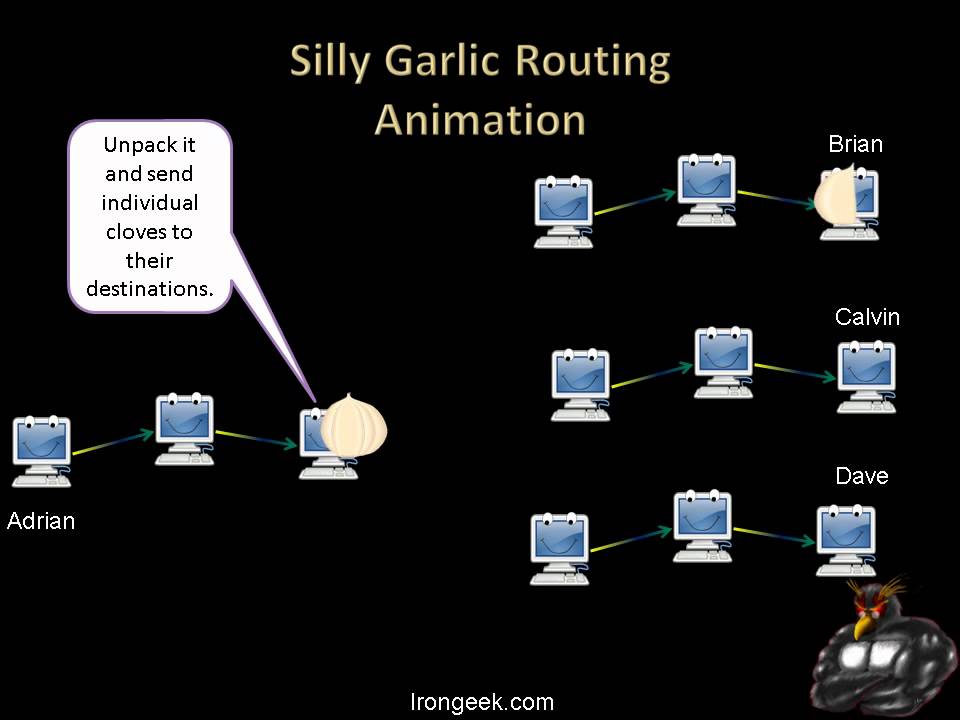
*Timing analysis* in the tor network is something that most of us fear when talking about TOR. When we browse the internet on the clear internet using our browsers all of our traffic can easily get logged and traced by our Internet Service Providers. Even if the traffic is encrypted the logs still exist. Traffic analysis searches records of connections made by a potential client and tries to match timing and data transfers to connections made to a potential server. If an attacker controlled the exit node he can see the amount of data transferred and the amount of seconds it passed since the server sent back those requests thus obtaining some information about the connection[12].

Another interesting attack is *the bad apple attack*, which is performed through BitTorrent. In this attack both the Ip address and the location of the client can be revealed.



Picture 14. Exit node eavesdropping

This can be mitigated by using another routing technique knows as *Garlic routing.* It was invented as an extension to onion routing, where multiple messages are bundled together, the so called “bulbs”, or garlic gloves. Each message has its own delivery instruction and they are exposed at the exit node and sent to respective addresses[15]. It encrypts multiple messages at once making it harder for the attackers to perform traffic analysis. By doing this it also increases size of the data transfer. Some applications that use garlic routing are I2P which is an anonymizing overlay network written in Java that allows other application to run on top of it. It is open source just like TOR.



*Picture 15. Garlic routing*

Also, some weaknesses of the TOR browser for example were kept in secret by the governments in order for them to get the upper hand. One extension called *NoScript* that blocks all JavaScript executing on the system when the browser is set to the highest security mode was actually vulnerable to JavaScript code injection, and let the attacker run any JS code on the target [14]. Although this problem was patched in the newer versions of the browser, it still remains a mystery for how long the attackers and the government could have used it for their purposes. Even though leaks are constantly being patched, you can never be sure whether that happens in time.

*Tor users are regularly hacked*. One thing that one should also consider is the amount of cyber criminals and hackers in general residing on the internet. Many forums offer links, files and many goodies which can be interesting for the everyday user. The whole dark web is swarming with malware and the security of the users is only as good as much as they themselves pay attention to it, and we know that social engineering is a number 1. Attack hackers use today.

So using the onion network without proper protection like VPNs, with Javascript, client side code and without good antivirus software is making your job only harder if you plan to stay anonymous or you want to protect your privacy. Generally using Tor is safe. In fact, Tor was created to browse the internet more freely, safely and anonymously, anonymizing your traffic by guiding it through different servers. However, Tor can be used for some riskier things as well, such as accessing the dark web. This is something which can pose dangers to be careful of.

***9. Conclusion***

In this research we covered some basic concepts of a more complex system that is onion routing, its usage, the way it helps people keep their privacy under control and ways other parties try to invade that privacy. As we become more digitalized and our systems we use everyday more dependent of the technology and the internet we will open holes to many vulnerabilities and security concerns when it comes to our privacy. Onion routing and onion networks are the things that help us keep this at bay. Being the open source project it is The tor project will remain open source until the end of it probably. This allows us as users to contribute to it in the best way we can, and we should definitely try to do this. Internet and it’s rules and protocols will surely keep growing and the time will come when we will have to grow along with it, in order to survive.

***10. References***

1. *https://www.torproject.org/about/history/*
2. *https://www.onion-router.net/*
3. *https://www.geeksforgeeks.org/onion-routing/*
4. *https://www.youtube.com/watch?v=QRYzre4bf7I*
5. *https://support.torproject.org/censorship/censorship-7/*
6. *http://cryptowiki.net/index.php?title=Onion\_encryption\_and\_its\_application\_for\_Tor\_anonymous\_communication*
7. *https://www.youtube.com/watch?v=o2BYWYS73G0*
8. *https://www.dictionary.com/e/dark-web/*
9. *https://www.broadbandsearch.net/blog/facts-about-dark-web*
10. *https://www.youtube.com/watch?v=lVcbq\_a5N9I*
11. *https://www.dailydot.com/layer8/what-is-dark-web/*
12. *https://latesthackingnews.com/2017/05/15/some-weaknesses-in-the-tor/*
13. *https://erainnovator.com/tor/*
14. *https://www.pcmag.com/news/tor-browser-has-a-flaw-that-governments-may-have-exploited*
15. *https://www.youtube.com/watch?v=NV90TRs\_pGE*