Halmstad University
School of IDE
Network Security 7.5 hp
Network design and Computer management

TOR

A way to stay private over the Internet

Spring term 2008

Tobias Persson
Kristian Löfvenholm
Linus Barkman

Table of Contents

Privacy *(noun)*
Someone's right to keep their personal matters and relationships secret
[Cambridge advanced learner's dictionary]

Introduction

Ever since the Internet became popular for "ordinary people", the words privacy and personal integrity have been more widely used than ever before. Articles about privacy and personal integrity are usually reflecting the risk of personal information leaking out from a government instance or some type of internet community, but there is a lot more to it.

The need for privacy over the years

Before the Internet peoples worries about integrity were mostly regarding a peeping Tom looking through the window into your home, maybe a burglar or someone not authorized looking at e.g. your medical record, which at the time would be locked up in a cabinet rather than in a computer database. People wouldn't worry about someone keeping track of where they each morning went jogging, where they did your weekly grocery shopping or where they were at any given moment.

It is safe to say that it is not very likely that someone keeps track of the above mentioned situations just because of the Internet, but in regard to the shopping and your whereabouts (when using the Internet) , these situations can be tracked straight back to you. "So what if someone tracks your surfing habits", you might say, "I have nothing to hide"… But, what if someone constantly looked over your shoulder while you were shopping, and in this way monitoring your shopping habits and finding out your home address? Would this be appreciated? Probably not, although this is possible over the Internet, ISPs' not rarely sell information about their customers surf habits to marketers, only for these marketers to be able to personalize ads directed to you [1].

Or imagine this: your ISP (by orders from the government) prevents you from looking up, or posting, certain things on the Web. A government trying to keep you from saying what you want or access the information you wish to have, in a non criminal way (i.e. not hacking into secure systems), is not letting you practice your right to information, one of the pillars of the Internet. It is also preventing you from practicing your freedom of speech which is on the list of Universal declaration of human rights[2].

After pointing out that it is not preferable to be monitored whilst on the internet for fully legitimate reasons, it is quite obvious that there are those who wish to stay anonymous to be able to commit illegal actions, such as breaking in to secure systems, perform identity theft or credit card fraud.

Are there things to do to keep a high rate of privacy and personal integrity whilst surfing the web? Well, there are tools that, if correctly configured, will mask your internet use

and minimize the possibility of tracking your IP-address. A very good tool to accomplish this is TOR (The Onion Router).

History and users

Tor was initially financially sponsored by the US Naval Research Library but became an EFF-project in 2004 and was financially supported until late 2005[3].

Tor was used by the American navy whilst stationed in the Middle East, primarily when collecting information, the American police are known to take advantage of the Tor network while investigating criminal organizations on the web. Journalists can see a possible use of Tor when communicating with informants, in this way not risking to give up what the informant is doing. Companies might take advantage of Tor to prevent industrial spies from analyzing network traffic destined outside the LAN.

This can be done since the usage of Tor will not reveal the source address, hence it is not possible for others to successfully trace the source back to someone[2].

How TOR works

Tor is an anonymous network who helps people become anonymous on the Internet. Tor sends traffic to all over the world and takes different paths all the time. It's hard to track someone who uses Tor because you are using relay servers in different countries and it's encrypted. If the connection is not encrypted, people can use traffic analysis against you. Usually you send a packet from your computer to the destination, but with Tor you are sending the packet to many relay servers and they send it to the real destinations. With the Tor technique it's really hard to track down the real IP address, if you have configured it right.

When you create a network with Tor you need to have encrypted connections through all the servers you are connected to. A relay server needs to know how to relay and with Tor they just know how to reach to the next destination; they don't know anything about the network.

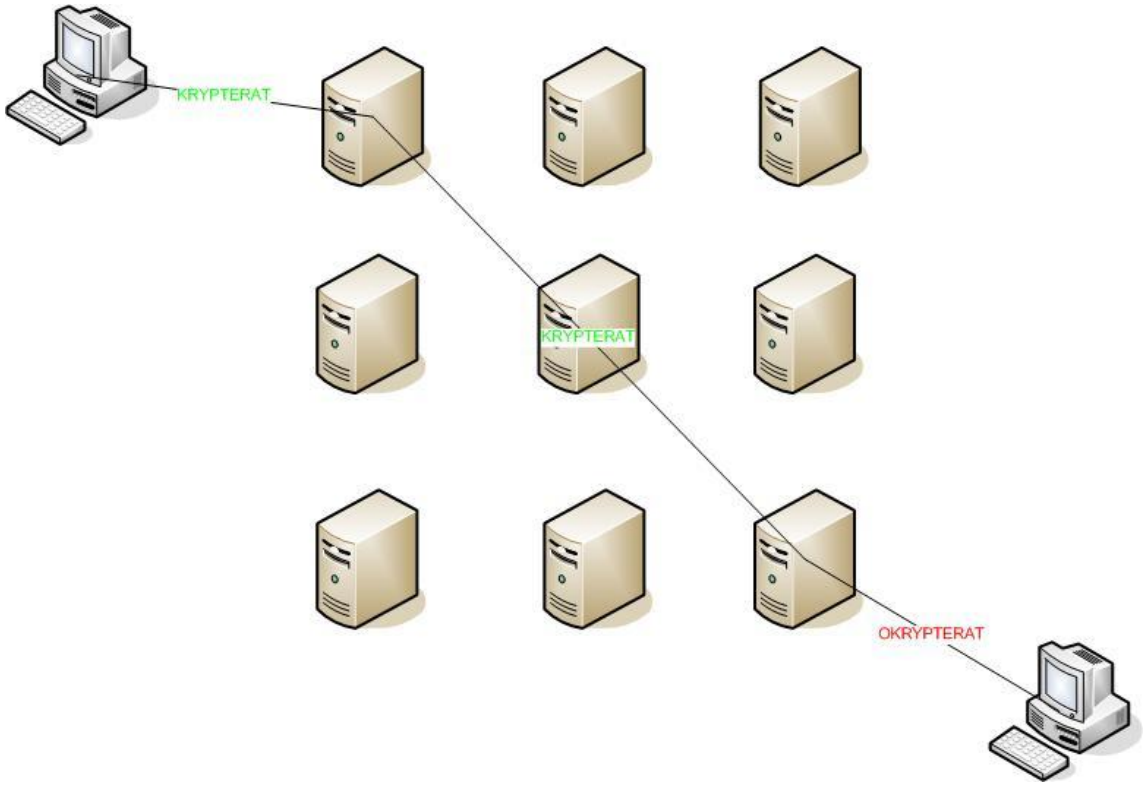

Figure 1: Tor encryption overview. Copyright Linus Barkman

A node-to-node connection is encrypted with TLS. Transport layer service (TLS) is a technique people are using between two TCP connections. TLS is using a symmetric encryption with message authentication code and it's common in e-commerce. Every Tor relay has a public decryption key and this is because they need to establish a secure connection between the relay server and the client. When the client needs to connect to the relay servers they search for servers in the Tor directory list. The directory list is full of servers and you can see the exit policies, approved relays, signed certificates, locations etc.

One of the best things about Tor is that you can't use any traffic analysis program on the relays because a relay server only sees one hop at the time. You can only use Tor with the TCP protocol and with programs that support SOCKS. You have the same routing path in about ten minutes and then you get a new path. [9, 3]

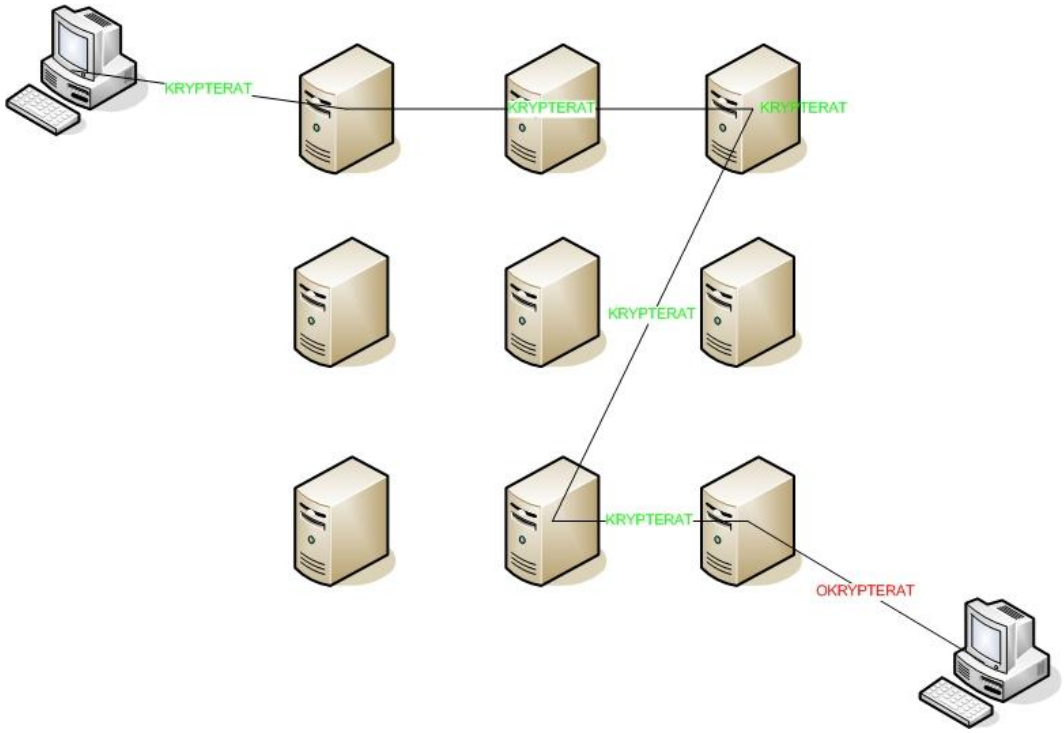

Figure 2: Tor encryption different paths. Copyright Linus Barkman

Why should I use Tor?

Because it will keep you anonymous on the Internet and you are not a victim of traffic analysis anymore, except if they can see both exit ends of the connection and do man in the middle attack (Eavesdropping by exit nodes). With traffic analysis you can easily see passwords, urls, instants messages and emails. Be careful and read your employment policy, some companies don't allow Tor or similar applications. This is because the companies can't use "traffic analysis" on you because you have established a secure connection between the relay server and they have no authority to see anything. Of course your supervisor wants to see that you actually work and that is why they have "traffic analysis". [3]

Eavesdropping by Exit nodes

A Swedish security consultant Dan Egerstad leaked over 100 secret passwords and mail accounts. It was accounts to governments and embassies world wide. Dan just made a MITM lab and got the accounts. He came over an email from the Swedish court to the Russian embassy, and it's confirmed from the Swedish court. Dan tried to contact some embassies and help them fix the problem, but with no luck. The last solution was to leak everything and hope they act fast. Dan was right they act fast, in November 2007 Dan Egerstad was arrested for publishing the information. Dan has the award of "hack of the year" and he got some publicity. [6, 7, 8]

Personal integrity

If you are living in a country that has censorship you can use Tor to access web pages which are blocked by your country's Internet Service Provider (ISP). In China they have censorship on many web pages about news, health, education and entertainment. China

even blocked Google in ten days but they reversed its decision. Google has exploded in China because you can search in Chinese language, and not just in English. Many Chinese people are using Google for research and education not for political reasons. [4, 5]

"Obviously there is some harmful information on the Internet" says the foreign ministry spokesman Kong Quan. [5]

Well he's right, but I don't think that closing down Google or any other search engines would help him to solve the problems. The search engines have so much positive things that you have to filter out the bad Internet sites; terrorism, how to make bombs/weapons, child porn and so on. Because of the Internet you can access information very easy and you are allowed to be on any websites if it's not illegal, you are allowed to have integrity. According to Mike Perry on his whitepaper, the Chinese Internet service providers are doing a MITM (Man In The Middle attack) on SSL (Secure sockets layer). MITM is a form of eavesdropping; when two people are connected with SSL they think they have a secured connection. With MITM a third person are able to listen to every packet they send and receive - he's the man in the middle.

Tor network weaknesses

There are actually no verified weaknesses in Tor but instead most of the weaknesses lie in the software used to access the network. This is often caused by clients connected to the Tor servers not being configured correctly by the user using it [10].

One weakness or security issue is that people can stay anonymous when doing illegal stuff or operations not allowed. One example is that you can make an online order in an e-commerce shop (e.g. buying computer parts) in another person's name with a false identification and a hidden real IP-address (further called just only IP for simplicity of reading). Now the company that you ordered the product(s) from is having a hard time tracing you [12]. Another example is when hackers trying to hack websites and/or web services with a false IP, or just people trying to get information about making bombs and such without being detected.

If you analyze Figure 2 you see that the communication to the end servers (e.g. google.com, microsoft.com, yahoo.com, …) are using unencrypted traffic at the Tor exit-node because they cannot understand the encrypted traffic that traverses the Tor network to and from the end users. So because of this there is a possibility that the traffic is monitored on the Tor exit-node which is decrypting the traffic to the servers [11].

Some administrators, sitting on the exit-node, monitor the traffic and filter out specific content (e.g. child porn) while some, I think, just snoop around to peek at what you are doing or are not monitoring anything at all. Because of all this information revealed to

others the anonymity of people using the Tor network is only relative. Why – because you cannot trust the person at the Tor exit-node to your final destination [13].

The Tor network is very slow because the bandwidth comes from people running Tor-clients (this is how Tor works in short words when the client is set to Onion Router-mode). This is a very big drawback to functionality of the whole network. Because of this sort-of-weakness it's almost only possible to surf the web or view your email without any delays. A study by Joshua Albrecht has more information on this big issue – with nice diagrams included in his report [13].

Is it possible to hack the Tor network?

Yes, it's possible to hack Tor but to manage that is not an easy task. But there's one important thing to know. When I talk about hacking Tor I mean trying to obtain information about the origin that initiated a request through the Tor network and thereby exploiting the anonymity of the person using it to fake his or her IP to the outside world.

I will not write about all available techniques. Instead I'm going to write about a technique called "phone home". With this you can make the client "phoning home" and ask "Who am I really" [10]. The "phone home" is about using protocols and client-side scripting that are common among almost all users browsing the web, such as JavaScript, Java, Flash and ActiveX [10][12].

"Rather than attempting to exploit weaknesses in Tor, we make use of technology that 99% of the people browsing the web will have enabled: JavaScript and Flash" ~ Andrew Christensen, Practical Onion Hacking p.4, [10]

One way of "phone home" goes through the Tor network and the second way is a method that sends and receives traffic outside the Tor network. There's an image in a paper written by Andrew Christensen [10] (Diagram 1) that describes the logic behind the technique. I'm going to describe the outside-method.

To make this work you need a web server with a website, which content you can change, and a Tor exit-node up and running to be able to insert a sort of bug that activates the "phone home" method. It briefly works like this [10]:

1. Victim connecting through the Tor exit-node, browsing a regular website.
2. Exit-node turns off compression and changes the HTTP headers sent to the website.
3. Exit-node modifies packets and inserts a HTML iframe (inline frame) that points to your web server and a recognizable cookie.
4. Your web server receives the Tor request via the iframe including the cookie value and then creates some JavaScript code that makes a GET-request to a non-existing image with the real hostname and IP included in the fictive image filename.
5. This JavaScript code is then sent back to the browser at the Victim's computer and executed to do the actual GET-request.
6. After this Flash is used in the Victim's browser to execute an outside connection (outside of Tor) thereby creating a direct connection. This is because Flash

doesn't use the Tor network (SOCKS protocol). It resends the cookie value and this allows a mapping between the real IP and the IP used including the website viewed in Tor.

Note that the JavaScript code found in the Practical Onion Hacking paper [10] doesn't work correctly anymore and needs to be tweaked. I personally tried modifying the script and tested it in my Firefox browser – and the results were that it worked. That was very scary if you ask me.

An example of the fictive image that doesn't exists and the cookie value can be seen here: http://COOKIE.unknown.website.se/VictimHostname_VictimIP.png. The first part is a technique used to make the Victim's host make a local DNS lookup for the given address, instead of letting Tor resolve the address for you. If the hack works successfully you can see the IP of the Victim or at least his or her registered ISP [10].

Other Threats

All this analysis (that I'm going to write about) can be used as long as the traffic isn't encrypted, which is at the Tor exit-node. There are ways of fingerprinting traffic by ways of traffic-analyzing. With this you can (not always) recognize and track the type and version of the web browser used to initiate website requests, if SSH or telnet is being used, SSL and more. Sometimes you're even able to get information about the operating system (OS) used just by looking at the packet headers and versions of the protocols used. Another key point is identifying the accepted language used by the browsers to maybe be able to identify the possible spoken language. Statistical analysis of information in end-to-end packets can also be used to determine the clients [12].

Protection against these hacks

Simply use a local firewall that is setup to only allow Tor traffic when Tor is being used. This prevents the use of techniques that tries to go outside of the Tor network and other malicious connections. Another effective tool is a proxy (such as Privoxy) that filters traffic before it is sent onto the Tor network [10]. You can also use Tor when in school or on a company to avoid revealing to true home IP. But if your Tor-connection can be traced to your account on e.g. the school network, then you're busted.

Conclusion

Tor is without a doubt, a very powerful utility that is freely available over the internet. The implementation and everyday use of Tor does not require major network knowledge by the end user, since there has been developed a practical GUI and a simple installation package which configures the host automatically. As described in this report there are some risks to take into consideration and the configuration of Tor is very important, or the whole point might be lost.

Since Tor is relying on nodes to forward the traffic, the connection is only as fast as the slowest link on the route. This is a major drawback resulting in the fact that Tor is not always reliable for everyday internet use when implemented by an IT-department, on

staff computers. This might be due to the fact that users get frustrated with the sometimes excessive loading times for web pages and therefore turn it off. Any it security system is only as safe as the user utilizing it, and the need to educate users how critical it is to the company is very important.

There is an ethical aspect to take into consideration when discussing Tor. Since it makes it possible for e.g. criminals to disguise themselves and commit crimes without risking being caught. Imagine someone stealing an identity and using it over the net with Tor, the possibility of catching this individual is not an easy task, since Tor is such a powerful cloaking device. So by using, developing and donating money to Tor are we involuntary supporting criminals possibility to perform their crimes?

As mentioned before Tor is used against criminality as both prevention but also to discover criminal actions that are being committed. As long as web developers work towards a safer environment for everyday usage not making it an advantage for criminals to hide themselves amongst the 1's and 0's in the interactive society, there would only be positive response to the use of Tor.

References

[1] http://seekingalpha.com/article/29449-compete-ceo-isps-sell-clickstreams-for-5-a-month (last accessed: 5th May 2008).
[2] http://www.un.org/Overview/rights.html (last accessed: 5th May 2008).
[3] http://www.torproject.org/ (last accessed: 5th May 2008).
[4] BBC News URL: http://news.bbc.co.uk/2/hi/technology/2540309.stm (last accessed: 6th May 2008).
[5] BBC News URL: http://news.bbc.co.uk/2/hi/technology/2254622.stm (last accessed: 6th May 2008).
[6] Computer Sweden URL: http://computersweden.idg.se/2.2683/1.118681 (last accessed: 11th May 2008).
[7] IDG URL: http://www.idg.se/2.1085/1.130629 (last accessed: 11th May 2008).
[8] The Sydney morning Herald URL: http://www.smh.com.au/news/security/police-swoop-on-hacker-of-the-year/2007/11/15/1194766821481.html (last accessed: 11th May 2008).
[9] Black Hat USA, Mike Perry URL http://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-perry-WP.pdf (last accessed: 8th May 2008).
[10] Andrew Christensen, FortConsult, URL: http://packetstormsecurity.org/0610-advisories/Practical_Onion_Hacking.pdf (last accessed 8th of May 2008)
[11] Mark Joseph Edwards, News editor at Windows IT Pro, URL: http://windowsitpro.com/article/articleid/94014/security-update--the-onion-router-downside--october-25-2006.html (last accessed 7th of May 2008)
[12] Andrew Christensen, FortConsult, URL: http://www.fortconsult.net/images/pdf/tpr_100506.pdf (last accessed 8th of May 2008)
[13] Joshua Albrecht, Computer Science student at University of Pittsburgh, URL: http://www.cs.pitt.edu/~jsa8/network_report.pdf (last accessed 8th of May 2008)