Online Security and Privacy Protection using HTTPS and Tor

Mritunjay Ojha[1] Aayush Pathak[2] Akshay J. Boramani[3] Danish K. Chaus[4]
[1]Faculty [2,3,4]Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Fr. C. Rodrigues Institute of Technology, Vashi, India

Abstract— While using internet, a lot of user information such as username/passwords, user location, browser history, data, etc is passed along the network. All these details are visible to the ISP (Internet Service Provider). This information can also be used by the hackers. Information is the most valuable asset. Thus, there is a need to protect the user information. This can be carried out by using https with tor browser. In this paper, we have analyzed the working of https with tor. This is a study paper which gives the working of https with tor browser to protect the user privacy. The different types of data transferred over the internet with and without https and tor is specified in the paper.

Key words: HTTPS, TOR, TOR Browser, NSA, Hacker, Sys Admin

I. Introduction

A. HTTPS:

Hypertext Transfer Protocol Secure (https) is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocol. TLS is an authentication and security protocol widely implemented in browsers and Web servers. The main motivation for HTTPS is authentication of visited website and protection of privacy and integrity of the exchanged data. [1]

B. TOR:

Tor is a circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points. Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency. [2][3]

C. Tor Browser:

The Tor Browser, previously known as the Tor Browser Bundle (TBB), is the flagship product of the Tor Project. It consists of a modified Mozilla Firefox ESRweb browser, the TorButton, TorLauncher, NoScript, and Firefox extensions and the Tor proxy. It can be run from removable media and is available for Windows, Mac OS X, and Linux.

The Tor Browser automatically starts Tor background processes and routes traffic through the Tor network. Upon termination of a session the browser deletes privacy-sensitive data such as HTTP cookies and the browsing history. [2][3]

D. NSA:

The National Security Agency (NSA) is an intelligence organization of the United States government, responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counter intelligence purposes, a discipline known as signals intelligence (SIGINT). [4]

E. SYSADMIN:

A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget. [4]

F. Background:

The organization of the report is as follows. Section 2 discusses about the working of internet without https and tor. The section 3 discusses about the data visible throughout the network when https protocol is used. Section 4 discusses the data visible when tor browsing is used. Section 5 discusses the use of combination of https with tor to provide security and privacy protection. Finally section 6 presents the conclusion.

II. Without HTTPS and Tor

A. Client Side:

Using normal unsecured internet browsing, whenever user accesses his email, or updates Facebook page, or checks bank statement, there are dozens of points at which potential adversaries can intercept the Internet traffic. [6] Information about the user such as browser history, username and password, location, data transferred, etc are visible throughout the network. This information is available to the ISP (Internet Service Provider) on the client side. A hacker can use man-in-the middle attack or eavesdropping to gain access to this information and thus use it inappropriately.

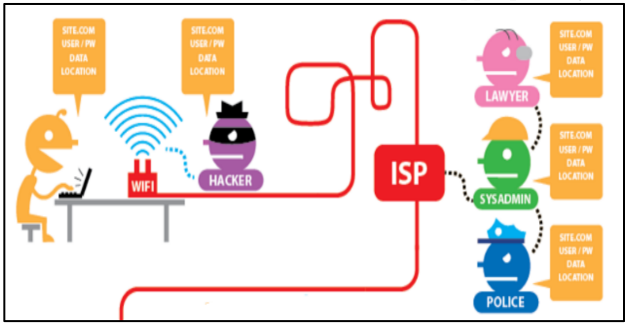

Fig. 1: Data visibility (Client side) [5]

B. Server Side:

All the information is also visible to the ISP present at the server side. The National Security Agency (NSA) can also easily access all the details about the user.

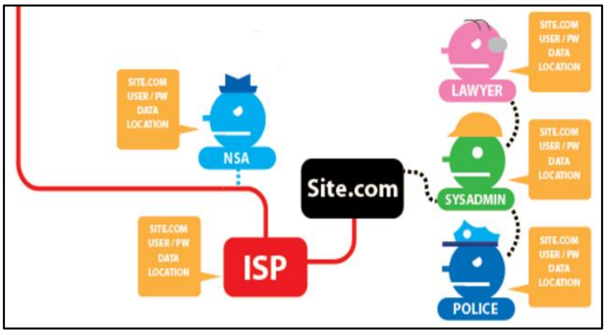

Fig. 2: Data visibility (Server side) [5]

III. USING HTTPS PROTOCOL

A. Client Side:

HTTPS encrypts the data and thus helps users gain considerable protection, most notably against eavesdroppers on wifi network and eavesdroppers on the network between user and the site being accessed by the user. [6]

Thus, when the hacker tries to access the user information, he can gain only the site details and the location of the user. Same is the case with ISP.

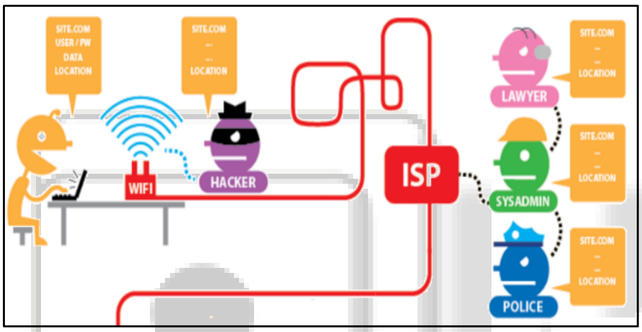

Fig. 3: Data visibility using https (Client side) [5]

B. Server Side:

At the server side, only the site and user location details are visible to the NSA and the ISP. Only the system admin, lawyer and the police have visibility to all the details of the user.

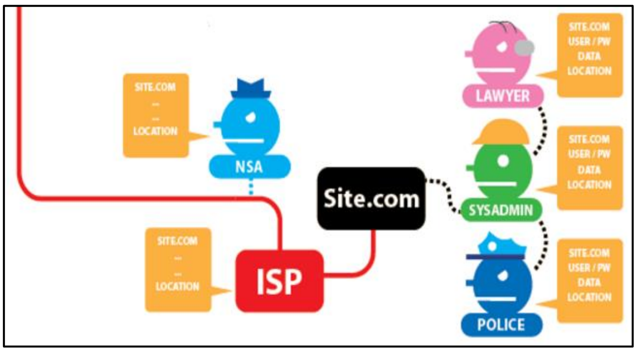

Fig. 4: Data visibility using https (Server side) [5]

IV. USING TOR

A. Client Side:

The tor browser helps to protect users anonymity online. [6] Using tor browser, all the details about the user are hidden. A hacker eavesdropping on the wifi can only see the location details of the user (i.e the origin of the request). The request (site details) are also not visible to the hacker or the ISP. Thus, using tor, user can access any website without the knowledge of the ISP. Since there is no node between the user (client) and the ISP, the user location is visible to the ISP.

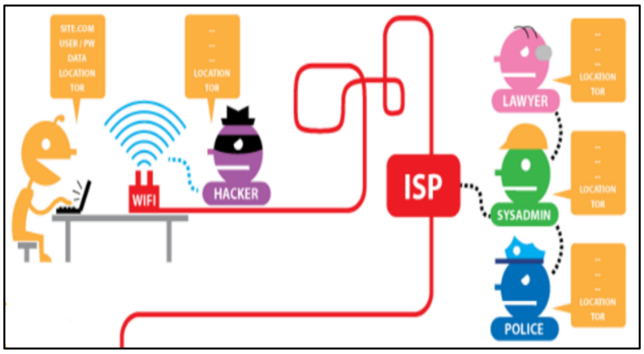

Fig. 5: Data visibility using tor (Client side) [5]

B. Tor Relay:

In tor, the request packets are transferred through various hops (relay nodes). At each such node, encapsulation takes place. Thus, at each node, only the location (address) of the previous node is visible. This makes it very difficult to trace the origin of request.

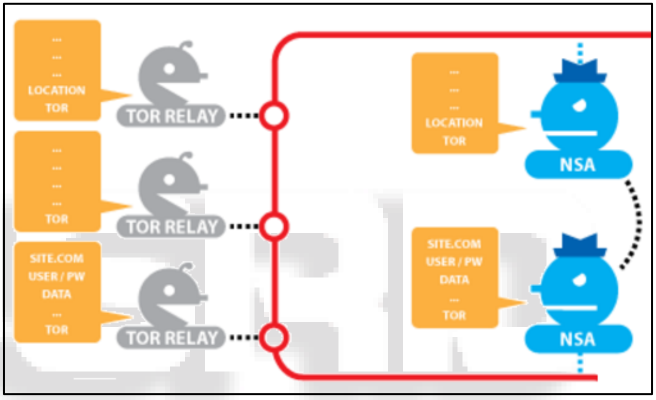

Fig. 6: Data visibility using tor (Relay Nodes) [5]

C. Server Side:

At the server side, all the information about the last relay node is visible to the NSA and the ISP. Thus this information is also available to the system admin present at the site server. Due to relay nodes, even the system admin is not able to gain information about the origin of the request.

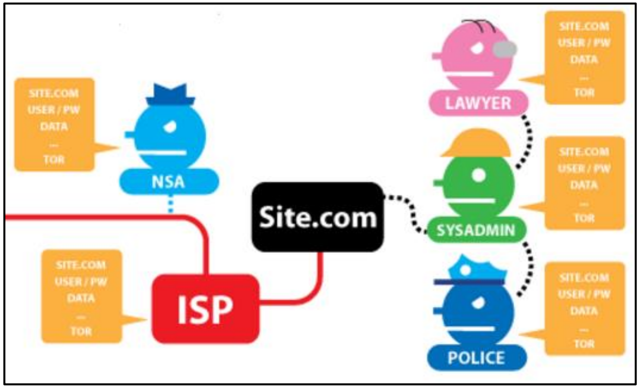

Fig. 7: Data visibility using tor (Server side) [5]

V. COMBINATION OF HTTPS WITH TOR

A. Client Side:

Using https with tor provides the highest level of security and privacy protection. The data visibility at the client side is similar to the visibility at the client side using tor. i.e Only user location details are visible to the eavesdropping hacker as well as the ISP.

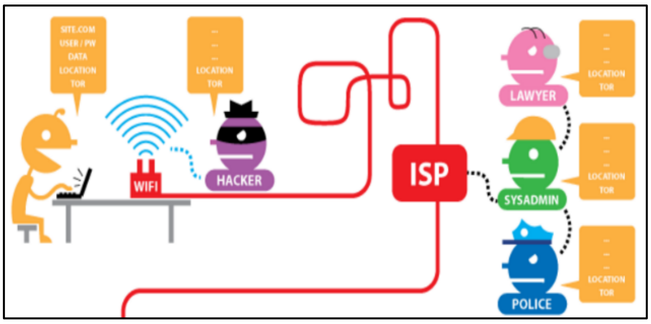

Fig. 8: Data visibility using https with tor (Client side) [5]

B. Tor Relay:

While using https with tor, there is a slight difference as compared to the working when only tor is used. In this, the last relay node does not store all the details of its previous node. It only stores the site details of the previous node.

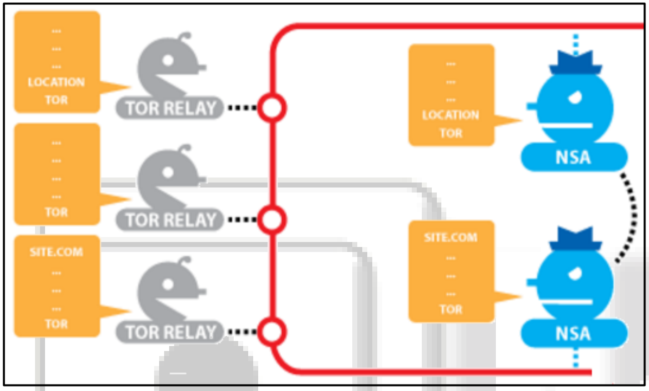

Fig. 9: Data visibility using https with tor (Relay Nodes) [5]

C. Server Side:

Since the last tor node stores only the site details, the NSA and the ISP present at the server side can gain knowledge only about the site request. The ISP at the server side does not have any other information visible to him. Only the system admin at the site server has visibility to other details. Due to relay nodes, the location details are not visible even to the system admin.

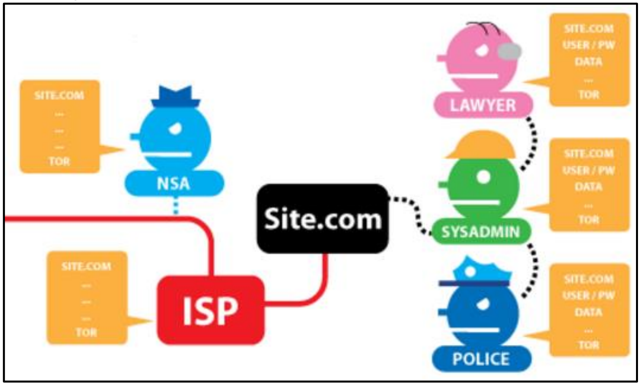

Fig. 10: Data visibility using https with tor (Server side) [5]

VI. CONCLUSION

In modern times, user information is the most valuable asset. Breach of user data can lead to loss of user privacy and security. Hackers can access this information and use it in some inappropriate ways. To prevent this and to provide internet users with privacy and online security, a combination of https and tor can be used. Https provides encryption of data so that the information is encrypted and secured from eavesdropping hackers as well as the ISP. The tor browser makes use of relay nodes to transfer the request packet from one node to another. At each node encapsulation is carried out. Thus, every node can have knowledge only about its previous node. Hence, the origin of the request can never be traced even by the ISP or the system admin.

Thus, using https with tor would provide data security using encryption provided by https and user privacy through tor.

REFERENCES

[1] Jeremy Clark and Paul C. van Oorschot “SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements” 2013 IEEE Symposium on Security and Privacy.

[2] https://www.torproject.org/

[3] Roger Dingledine Nick Mathewson Paul Syverson “Tor: The Second-Generation Onion Router”

[4] https://en.wikipedia.org

[5] https://www.eff.org/pages/tor-and-https

[6] https://www.eff.org/deeplinks/2012/03/https-and-tor-working-together-protect-your-privacy-and-security-online