A Survey on Defensive Mechanism of Eclipse Attack in I2P

[1]Hasib Vhora,[2]Mr. Girish Khilari

[1]IT Systems & Network Security,
[1]Gujarat Technological University, Ahmedabad, India

***Abstract* - The 'Darknet' is a part of cyberspace that is hidden from the 'surface web'. In Darknet both publishers and visitors are anonymous. There are several ways to access Darknet such as through Freenet, TOR and I2P. Though I2P is a decentralized anonymous network, there are several security risks incorporated with Distributed Hash Table (DHT) that may breach anonymity of I2P. In this paper, we will study basics of I2P, Eclipse attack and Existing defense mechanism of Eclipse attack. By this study we can discover strong mechanism to prevent Eclipse attack.**

***Index Terms* - Invisible Internet Project, Attacks, Eclipse Attack, Defense mechanism**

I. INTRODUCTION

A darknet is a non-private network in which connections are made only between trusted peers which are also known as "friends". As sharing is anonymous, Darknets are separate from other distributed P2P networks and therefore users can communicate with little fear of governmental or corporate interference.[9] Within the darknet both web surfers and website publishers are entirely anonymous. This anonymity is usually achieved using an Anonymous Networks.I2P provides more anonymity to users. It is basically for the people who care about their security.I2P is used for file sharing and storage, blogging and chatting.

This paper organized as follows: Section II briefly discuss about Invisible Internet Project (I2P). Section III describes Eclipse Attack. Section IV discusses existing defense mechanism of eclipse attack. Section V draws some conclusions.

II. INVISIBLE INTERNET PROJECT

Invisible Internet Project is an anonymous overlay network. It is a network within a network. It is intended to protect communication from monitoring by third parties such as ISPs. No network can be completely anonymous. The continued goal of I2P is to form attacks harder to mount. Its anonymity will get stronger as the size of the network increases.[8]

I2P exposes a layer which applications can use to send messages securely and anonymously to each other. Communications in I2P are end to end encrypted. The endpoints of all communications have their own cryptographic identifiers.

I2P is self organized network and it is also resilient and scalable packet switched anonymous network layer on which different anonymity or security conscious applications can run. Each of these applications can create their own latency, anonymity and throughput without concern regarding the correct implementation of a free route mixnet, permitting them to mix their activity with the larger anonymity set of users already running on top of I2P.Applications of I2P are anonymous web browsing, web hosting, chat, file sharing, e-mail, blogging and newsgroups.

III. ECLIPSE ATTACK

In Eclipse attack, a set of malicious and colluding nodes arranges for a good node in such a way that the good node can peer only with malicious nodes. So the union of malicious nodes together makes a good node fool by writing their addresses into neighbour list of good node. By Eclipse attack, the attacker can control significant part of the network and divide the whole network into different subnetworks such that node in one subnetwork can communicate with node with other subnetwork through malicious node only. Eclipse attack can also be considered as high scale MITM attack.[1][2]

Relation between Sybil attack and Eclipse attack

In Sybil attack, a single malicious node possesses large number of identities in the network to control some part of the network. If attacker wants to continue sybil attack into Eclipse attack, the attacker will try to place the malicious nodes in the strategic routing path in such a way that all traffic will pass through the attacker node. However the Eclipse attack is possible even if there is a defense against the sybil attack such as certified node identities.[2]

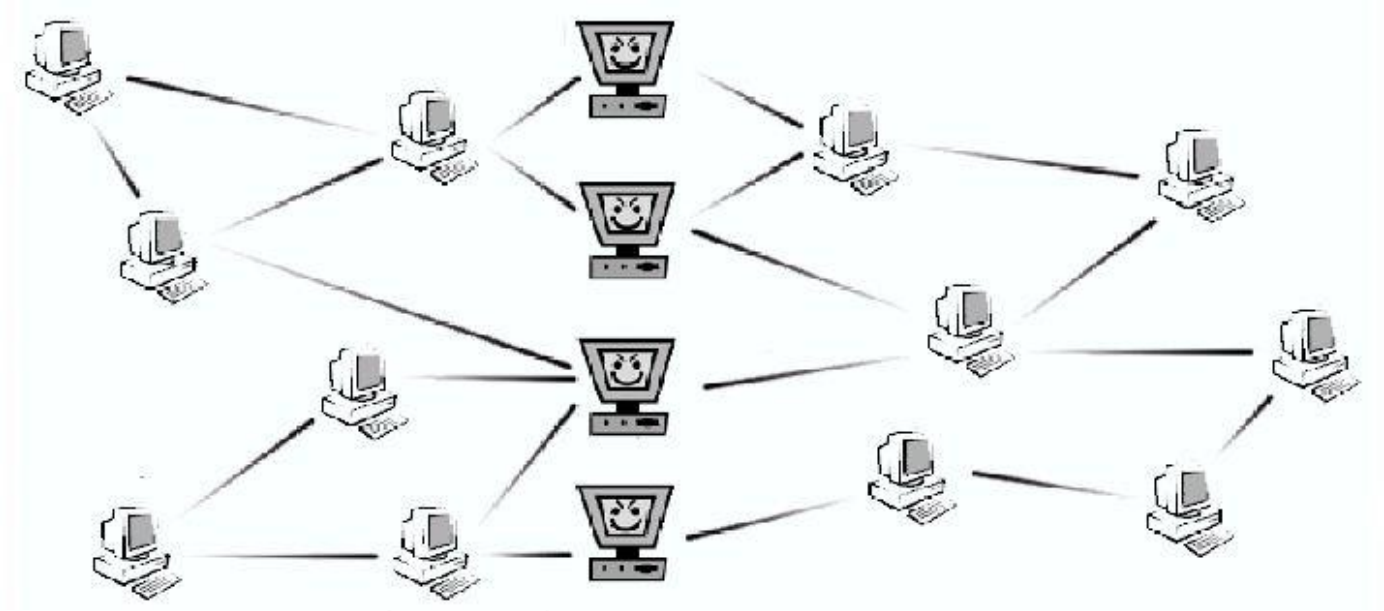

Figure 1 Eclipse Attack[2]

Impact of Eclipse Attack on the Network

The control pane can be attacked by the attacker by inefficiently rerouting the messages. If attacker decides to drop all the messages then the network will be divided into subnetworks. The attacker can inject the polluted files or request polluted files on behalf of good nodes so that the files will be copied along the way. In the DHT based networks, the neighbour information propagates to other peers also so a small number of malicious node are sufficient to do an Eclipse attack.[2]

IV. EXISTING DEFENSES AGAINST ECLIPSE ATTACK

Self registration algorithm[3][6]

It is the procedure for the new node to join in the network. In this procedure the existing nodes called "Registration Nodes" will check for the validity of the new node. It will greatly reduce the possibility of Sybil attack so that the possibility of Eclipse attack based on Sybil attack also decreases.

Defining indegree and outdegree bound[3]

This defense is especially for countermeasure of Eclipse attack. We bound the "indegree" and "outdegree" of the nodes in this defense.

indegree - number of direct routes coming into a node
outdegree - number of direct routes going out of a node

Problems identified in the existing defenses

In self registration algorithm the problems are,

1. Overhead on the registration node increases due to the joining requests of the new nodes.
2. No mechanism to authorize the registration node.
3. It causes "False registration" if malicious node involves in the registration process.[6]
4. It cause deanonymization of node because of reverse hash process.

In indegree and outdegree bound the problems are,

1. The malicious node can sometimes poisons the good node and can manipulate the indegree and outdegree bound.[6]
2. Recursive query can affect the performance.

V. CONCLUSION

We have already studied some existing defensive mechanism to mitigate Eclipse attack, but these do not provide complete protection against attack. Although I2P is designed to withstand attacks, the possibility of attacks like Eclipse is still there.

We can make the defense more powerful by using structured overlay network instead of unstructured network, comparing the routing tables before adding a node into a neighbor set of a node and limiting creation of identity.

VI. ACKNOWLEDGMENT

I would like to thank to all who supported me and guided me throughout the survey. I am very thankful to them. It was impossible to complete this without them.

REFERENCES

[1] Christoph Egger,Johannes Schlumberger,Christopher Kruegel and Giovanni Vigna, “Practical Attacks Against The I2P Network” – UCSB Computer Science (https://www.cs.ucsb.edu/~vigna/publications/2013_RAID_i2p.pdf),2013

[2] Atul Singh, Tsuen-Wan “Johnny” Ngan, Peter Druschel and Dan S. Wallach, “Eclipse Attacks on Overlay Networks: Threats and Defenses” - INFOCOM 2006. 25th IEEE International Conference on Computer Communications, April 2006

[3] Yu Yang and Lan Yang, “A Survey of Peer-to-Peer Attacks and Counter Attacks” - Proceedings of The 2013 World Congress in Computer Science (http://www.worldcomp-proceedings.com/proc/p2012/SAM9754.pdf), 2006

[4] L. Wang, Attacks Against Peer-to-Peer Networks and Countermeasures. TKK T-110.5290 Seminar on Network Security. Helsinki University of Technology, Finland, 2006.

[5] Dinger, J.,Inst. fur Telematik, Karlsruhe Univ., Germany, Hartenstein, H., “Defending the Sybil attack in P2P networks: taxonomy, challenges, and a proposal for self-registration”- The First International Conference on Availability, Reliability and Security, 2006. ARES 2006

[6] Mashimo, Y., Yasutomi, M., Shigeno, H., “SRJE: Decentralized Authentication Scheme against Sybil Attacks”- International conference on Network-Based Information Systems, 2009. NBIS '09

[7] Hari Balakrishnan, M. Frans Kaashoek, David Karger, Robert Morris, Ion Stoica, “LOOKING UP DATA IN P2P SYSTEMS”- at http://csis.pace.edu/~marchese/CS865/Papers/balakrishnan_p2p_cacm03.pdf

[8] Structured Peer-to-Peer Architectures, http://csis.pace.edu/~marchese/CS865/Lectures/Chap2/Chapter2a.htm

[9] The I2P , https://geti2p.net/en/docs/how/tech-intro