Poster: A Novel P2P-over-Zeronet Anonymous Communication Platform

Jinli Zhang[1], Junwei Su[1,2], Di Wu[1,2]
1 (Institute of Information Engineering, Chinese Academy of Sciences)
2 (School of Cyber Security, University of Chinese Academy of Sciences)
zhangjinli@iie.ac.cn, sujunwei@iie.ac.cn, wudi6@iie.ac.cn

***Abstract*—As people pay more attention to anonymity threat analysis, many existing anonymous communication tools are proved to be not robust enough. Effective anti-anonymity attacks are used to intercept or track them. In this work, we designed a novel P2P-over-Zeronet anonymous communication platform which uses a two-layer-P2P protocol. It doesn't need any directory service Infrastructure, and is built on zeronet, which composes of thousands of decentralized P2P(peer to peer) websites, and finally constitutes a P2P-over-P2P circuit. We will introduce three core modules of the platform and the P2P-over-P2P structure in detail. Many field tests will be done to prove that our platform is a reliable secured anonymous communication tool which can be applied to many location-sensitive network operation scenarios.**

Keywords—anonymous communication network; P2P-over-P2P; zeronet

I. INTRODUCTION

The increasing network surveillance and censorship have made anonymous network receive much attention. Tor[1] and I2P[2] have always been the most popular low-latency anonymous network. They either use onion router or DHT (distributed hash table) protocol to hide users' location (i.e. IP address). They provide an anonymous Internet access, but they are inevitably challenged to be deanonymized by effective attacks. In this work, we will propose a novel secure anti-tracking "P2P-over-Zeronet" anonymous platform using a two-layer-P2P protocol.

Lots of application software are using P2P protocol, including file distribution software such as BitTorrent and eMule, voice service software such as Skype, streaming media software such as PPLive. P2P protocol has no trusted central party and has better scalability; it avoids suffering from a central point of failure. It delivers data from one peer to more peers based on methods such as DHT. Even if a single peer is broken, the whole network will not be affected.

Zeronet is a decentralized website using Bitcoin cryptography and BitTorrent technology, which aims to build a censorship-resistant network[3]. It likes the network of peer-to-peer users. Users can sign and publish their own websites and visitors can choose to serve it by storing the source code to the local host automatically, until the files are deleted manually. The volume of the websites is less than 10MB, lightweight. It means that after visited by users all over the world, the websites will be hard to be shut down. All nodes serving the site will be updated incrementally and automatically when the original zeronet site is updated.

II. ANONYMITY OVERVIEW

Anonymous network not only guarantees anonymity of communication content, but also the entities of senders and receivers, which the Internet did not involve at first. But content encryption is not enough, as ordinary users need to protect personal privacy, business organizations need to ensure network security and government departments need to resist traffic analysis to prevent information disclosure. So a secure anonymous network is necessary.

Measuring an anonymous network always meets the following properties: 1) The location of the user is anonymous. 2) The relationship between the sender and receiver is uncertain. 3) It is anti-tracking and anti-forensics. 4) Communication content is best to be anonymous. Our platform has achieved all of the above. It hides the user's location by relaying many hops and the receiver does not know the sender's information. The hops consist of decentralized irrelevant websites and utilize two layers P2P network, which guarantees anti-tracking and anti-forensics. We also encrypt communication content to ensure privacy security.

III. DESIGN

Our platform designs a "P2P over P2P" structure to relay data hop-by-hop over volunteer nodes. The core function of first P2P layer is just like the onion router of Tor[1], by which we use to select n super nodes. The second P2P layer is directly utilizing zeronet's decentralized P2P website structure and functional methods. Our volunteer nodes are not provided by person or organization, but by non-cooperative zeronet websites all over the world which only need to provide browsing normally.

The platform consists of three modules: local editor, secure transfer module, and remote receive module (Figure1).

A. Local editor

It is in charge of configurations for users, helping users to process packets, including split, group and encode packets. It also encrypts packets content according to demand like HTTPS. Then following the core algorithm we designed, it selects n nodes in a pre-figured zeronet peer pool to relay data and it can automatically decide the hopping order of peers. Finally, the

application visits the first zeronet peer configured, and transfers the encrypted packets by the API of the secure transfer module.

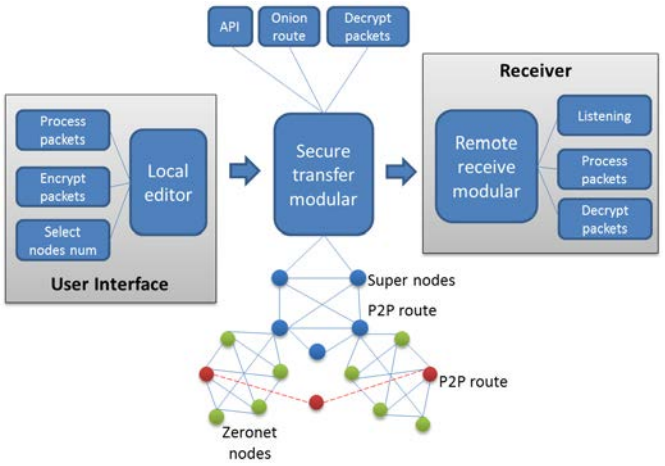

Figure 1: Platform architecture

B. Secure transfer module

The secure transfer module is embedded in the original zeronet sites we created. If someone visits an original zeronet site, visitors will store the site source code locally and the site can be visited by others based on zeronet's decentralized P2P mechanism. So the secure transfer module will be transferred from one peer to more peers in the P2P network all over the world.

Firstly we created many zeronet websites as super nodes (the blue tag zeronet nodes in Figure1) in the first layer P2P network. Every site keeps a dynamic list of zeronet peers. The zeronet website only url like http://127.0.0.1:43110/1HeLLo4uzjaLetFx6NH3PMwFP3qbRbTf3D is used as a neighbor information to contact other peers. According to the configured number of nodes, we select one zeronet as the first node and the number reduce one, then it contacts next neighboring peer by leveraging P2P selection algorithm until the number reduce to zero. When selected, the zeronet website will update its content, then it signs and publishes content by default to 5 nodes serving our original zeronet site (Figure 2). Zeronet maintains a user list including all users who visited and served the site. Zeronet can contact all users with user list by utilizing its namecoin mechanism.

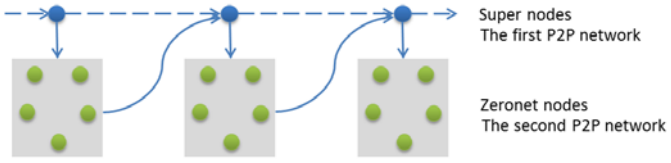

Figure 2: Two layers P2P network

Then we enter the second layer P2P network, whose peers consist of zeronet sites (the green tag zeronet nodes in Figure1) serving our websites. When the super zeronet node publishes to 5 nodes randomly in the update phase, we select a linkable peer as the real first node. Now we determine the first relay hop and it inherits its super node's selection which can contact the next super node. Then the next super node will select its P2P zeronet peer as the real second node which is determined as the second relay hop and so on. When all relay hops are determined, we create a hop-by-hop circuit (the red tag zeronet nodes in Figure1). As the zeronet sites are visited by others, the next update phase will choose 5 various publishing nodes.

When all nodes are determined, users can select a pre-figured algorithm to encrypt packets using Tor onion router. In the circuit path, each node only knows its predecessor and successor, and none of them knows all addresses.

C. Remote receive module

The remote receiver turns on a special port listening the incoming messages from other zeronet peers. It receives the grouping packets, and then processes them including regrouping and decoding them, as well as decrypting packets.

IV. Analysis

In this platform, the address of the next relay is neither an IP address nor a node ID, but a zeronet url. If hostile visitors intercept the data traffic, they cannot find any IP address, and the zeronet uses the namecoin mechanism to convert into a worldwide IP to pass data. Though the number of url alternative (for example we create 150 zeronet websites) is less than the Tor relays, but IPs of each url are more and are located anywhere. Moreover, any zeronet peer is distributed all over the world and website is almost impossible to be shut down.

Our platform relays data by two layers P2P network, so it is hard to be tracked. When one zeronet url is intercepted, it neither affects other zeronet url peers (super nodes in first layer P2P) nor the second layer P2P peers. Our zeronet websites consist of many different and irrelevant websites that have the same functions of store, encryption and forwarding. This guarantees enough anti-forensics and anonymity. Even if one zeronet is compromised, other websites are not correlated by providing normal browsing function. The zeronet sites which server for the second layer P2P may be online or offline randomly which cannot be exploited and tracked easily.

V. Conclusion

This work we design a novel anonymous platform with two layers P2P network combined with zeronet. The platform can achieve the purpose of anonymity, anti-tracking and anti-forensics. We believe it will be used for any identity-sensitive scenarios, such as botnet or ransomware command & control, after all, they have been used Tor to hide C&C server.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments for improving this paper. This work is supported by the Beijing Municipal Science & Technology Commission (No. Z161100002616032).

References

[1] Dingledine R, Mathewson N, Syverson P. Tor: The second-generation onion router[R]. Naval Research Lab Washington DC, 2004.

[2] Zantout B, Haraty R. I2P data communication system[C]//Proceedings of ICN. 2011: 401-409.

[3] https://zeronet.readthedocs.io/en/latest/.