Analysis of Attacks and Security Issues on the Peer-to-Peer Networks

Khalied Shredeh
Department of Computer Science,
University of jeddeh, KSA
branch al-kamel

ABSTRACT

Here in this paper we will review p2p network security issues, which is the subject of serious consideration should be given to him a full and carefully examine the condition of a people here will p2p system structures and attacks that may occur to p2p networks, as well as the potential for these attacks antibiotics and we will review the security issues that are in the routing Home p2p protocols and we will solve the major problems that occur in the exchange of files and applications on the network p2p process .

Keywords

P2P Network, security issues , attacks on p2p network , DoS attack, poisoning attack

1. INTRODUCTION

Over the recent period of growth, peer-to-peer to form a stunning and dangerous network evolved because it is considered as a means to mobilize resources for Internet users there became many systems of peer-to-peer, which enjoyed tremendous popularity in recent years systems because it has become a way of users to get anything without paying for it and here This research will provide some of the basic concepts of peer to peer systems and we will analyze the regulations and the types of attacks that attack the peer to peer network.

Here we will talk about networks, which consist of two types, namely the client networks and peer-to-peer in the formation of customer service will be the implementation of a specific task servers in the network may be a database server or a server or a secure server .

The model p2p comfortable model for the ability to search for files across the network using any form of centralized servers clustered with him as the central node in addition to the hybrid p2p networks and also there pure p2p networks do not have any central node and all transfers occur between users .

In addition, there are a number of security issues that occur in the p2p networks when designing a new application for network p2p must publish the code for them and in the current p2p systems must access the code to implement p2p system that is working properly and usually servers have the full features to reach the network hard drive that It allows users to create an operational code Systems p2p

2. DEFINATION OF P2P

P2p network is a special type of computer that behave self-regulation system and networks are self-organizing network does not have the resources and the centrality of that is the ability to link distributed throughout the network. Network p2p model and is in complete contradiction with the customer service network is a model of peer-to-peer best customer network model they be ready to distribute information considered networks have large spaces and unique in linking different p2p systems and also be heterogeneous with each other

3. BACKGROUND OF P2P NETWORK

In 1969 it established the idea of a network p2p in the first RFC comments and this means the host connection to a random host in customer service in addition to that was the first to get them to a P2P network from all Member In 1979 P2P network evolved while the user tries to access resources through each other In late 1990, has become here quite popular and a great network of peer-to-peer applications on file sharing users and exchange of multimedia and some examples of this in the most popular sharing in Freenet, Napster, Gnutella, Direct Connect, and BitTorrent In the latest estimates of the users sharing the file operation for more traffic any other application on the Internet and the recent rise of research and experiments in the field of p2p file sharing is the most popular in all fields Here are the most influential development of p2p protocols .

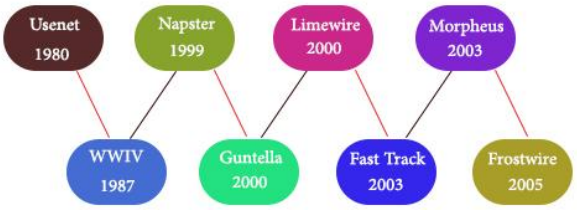
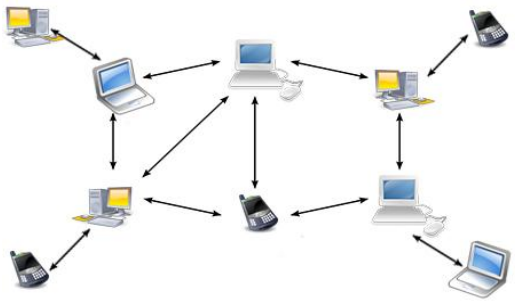


Fig 1 : Stages of the development of peer-to-peer network protocols

4. PEER TO PEER NETWORK CLASSIFICATION

There are several ways to classify peer networks to peer will talk about the first category is a approach which is used in network p2p applications such as file sharing and telephony as well as the media and the second approach is given a central in dealing and differentiate between pure p2p without a central server and networks with server information is stored in it peer and how to contract with one another link within the overlay network and how they are indexed items and we can classification networks to unstructured and structured



(Fig 2) Peer-to-peer network Classifications

4.1 Structured P2P Architecture

Structures p2p network regular is a network that uses private structures for the appointment of colleagues and the data elements and the presence of wrong with the title of allowing a unique type of data to peers given the current situation so as to ensure retrieval of data between peers, as well as the responsibilities that must be distributed in a manner specific and particular to understand the nature and function of the Directive distributed data and relies on the hash table is used to grasp and retrieve the key value Therefore, it is to include the removal of the key be net network responsible for the network key, as is the case in p2p organized networks using peer maintains on all pairs of keys and be worth to get the full library key other than buildings p2p irregular are determined and distribution data accurately through an infrastructure that provides recovery guarantee to search for data elements are indexed from within the network .

4.2 Unstructured P2P Architecture

Unstructured peer-to-peer networks is the networks do not impose a specific structure on the network, but formed connections before the contract with each other randomly and there are examples of Unstructured peer to peer network such as Gnutella, gossip, , and Kazaa and these networks behave approach is a specialty decentralization Engineering where they are peer transfer to neighboring peers in an effort to determine the active and important sites on the network in order to avoid the loss or loss of peer to peer network is moving all messages to all other peer-peer known whether this data was recorded or not

5. ATTACK ON P2P NETWORK

5.1 General Attacks and Defenses

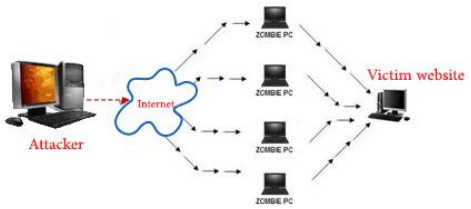
5.1.1 Dos and DDos attacks

Denial of service attack is an attack on the computers or computer network that cause the loss of a service and there are many forms of it, or are many ways to commit this DOS attack this in the case of P2P networks and is the most common form is to try to network flooding in fake package and thus prevent passage the network also used another method is to sink the victim in the account so that it is busy to respond to any inquiries are DOS attacks are more productive if they are to involve many of the hosts in the attack, and will talk about the DDOS attack is often the target of personal computers with broadband connections by a virus or Trojan horse and some control over these machines directed an attack on any host in the network .

In the end the targeting of non-harmful to the host via the speakers in the DDOS attack[2]. and is sending Unsatisfied malicious hosts is fool for an IP address to the IP of the victim and of course the process is a response from the host by sending packages to respond to the victim and knows this a reflection attack .

Defenses

Here we will talk about the technique used to block DDOS attacks on a large scale, namely, (pricing) here you will submit puzzles to his clients before continuing to the desired account and thus ensuring that clients go through expensive both accounts are DOS attacks are most effective when consumed most of the victim's resources striker and that in a bid flooding the victim's results and that the need to solve the mystery, he exclaims this attack is successful attack (pricing) because when the host is aware that under the attack gives a lot of puzzles that will be more expensive and thus reduces the impact of attacks despite the fact that this method is very effective against a number few of the attackers at one time distributed these attacks may fail and there are other disadvantages is that some customers believe that these puzzles are very difficult in mobile devices because it has lost battery power

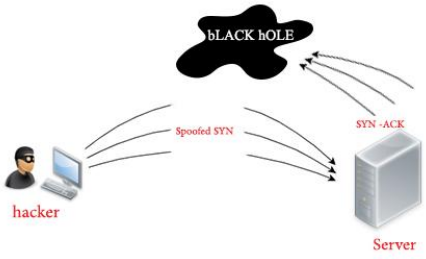


(Fig 3) Denial of service attack

Dos attack resist the victim node to provide the requested services and the performance of network decreases. So P2P networks are vulnerable to Dos and DDos attacks like TCP Syn flooding and Query flooding attack.

5.1.1.1 TCP Syn flooding attack

The TCP Syn flooding attack is Also Known As half attack TCP Syn because all requests are still in a state of half attack and through this is a way to repel this attack because when the server gets on TCP Syn on the package and signs of encryption and encryption of some of the security values such as the IP address of the client and the port number for a serial value because when the server is to receive the latest artificial demand, the responses of SYN + ACK in the previous process is not Server allocation in the data section and that when the ACK server receives and is verified ACK before retail is compared with the sequence value, but if this value is the same and is allocated server data segment with a TCP connection and the reduction of SYN cookies, which to be certified on the operating system as in Linux



(Fig 4) TCP Syn flooding attack

5.1.1.2 Query Flooding Attack

The query flooding attack is happening in the application of some p2p network pure layers such as Gnudella and thus obtain the required files and is broadcast query to all the neighbors and there are malicious knots are generating inquiries to flood the network as much as possible because if the DDoS query flooding attacks in the central p2p networks such as Napster, the damage will be greater Napster in the network have a lot of malignant colleagues which sends queries to the index server and so the traffic difficult on the server

There is also a group of attackers who intend to attack the victim sends the IP address as the source and you send inquiries popular files and be addressed to contain the files are another group of peer distributed and is sending an imaginary title to all colleagues and that means to be a victim of the large amount of responses from different servers, but follow the same movement and non-distributed query flooding attack can not solve this problem easily and that the small number of queries for each attack, the victim does not do any response to block traffic but the total amount of inquiries for the attackers may turn out to be a disaster

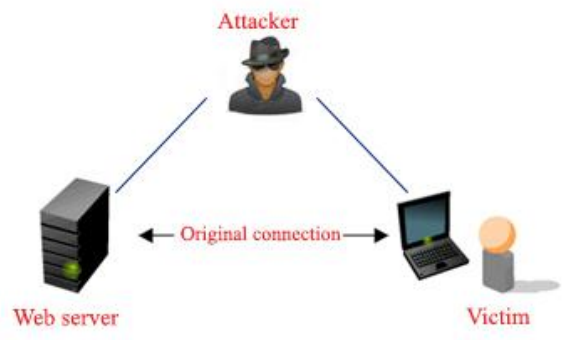
5.1.2 Man in the middle Attack

In a man-in-the-middle attack the center of the attacker introducing himself between two nodes in the process of choosing to stay in order to be spying on communications or manipulation more can be achieved by inserting or re-broadcast the previous messages in the data flow and thus can be for humans to achieve a set of goals . Man in the middle attacks therefore rely the protocols and are in many cases by impersonating the identity or send false information and is considered the attacks a man in the middle is a nightmare in most protocols

Finally, these attacks are less interesting in p2p networks is called at the same time cleansing and be identity spoofing in reducing traffic and application p2p supports various approvals between contracts and rely man-in the- middle attacks, on the same protocol and be potential attacks publish contaminated files in the network entity

Defenses

Without a central trusted authority, which generally do not exist in P2P networks, it is not possible to detect a man-in-the-middle attack. Nodes have no information about their neighbors and have no way of being able to identify them later with certainty. Fortunately, as man-in-the-middle attacks are mostly useless in P2P networks, this is not very alarming news.



(Fig 5) Man in the middle Attack

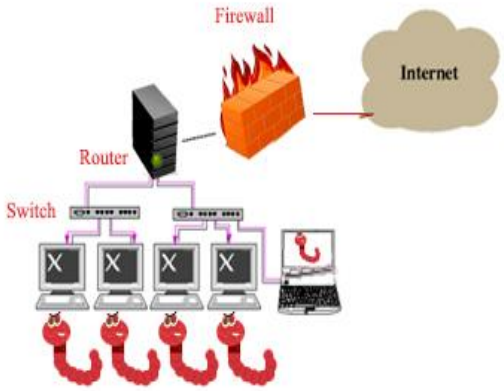
5.1.3 Worm Propagation

Worms is currently the biggest challenges on the Internet because the worms are considered capable of infecting hundreds of thousands of troops within hours, such as Code Red or Nimda worms engineered and be able to pass the infection in a few seconds and you will be worms in p2p applications would be disastrous and perhaps more threatening There are several factors which make P2P networks attractive for worms :

1. P2p networks made up of computers and the operating system one and therefore an attacker could be the entire network breach in an attempt to find one security gap that could be exploited
2. P2p applications used to transfer large files, although the size of worms, it is doing a node in a TCP packet and this problem will not be in the p2p network again, and can therefore be more complicated thing for taking behaviors
3. It is run p2p programs on personal computers instead of servers and thus be more likely an attacker to obtain sensitive files such as credit card numbers and passwords

Defenses

There must be awareness network users p2p not leave the PC without a monitor from a wall full protection and program to combat viruses on the Internet Perhaps the solution is for developers p2p software not write needles program bugged and this elusive goal, but it would be better for the benefit of all Java languages or c ++. – p2p network hybrids are considered to have weakened with the pure point p2p systems so as to make some more property contract with others to have the possibility to target the strategic deployment of the contract instead of worm more efficient at a later time



(Fig 6) Worm Propagation

5.2 Specific P2P Attacks and Defenses

5.2.1 Rational Attacks

Must be cooperation and collaboration between p2p services to be effective, but in most cases represents a node of one party and be self cooperation and interest are also subjective and but there are a large part of the contract p2p rational and trying to adapt to the system resources to maximize consumption through the use little for themselves because he if they were a large number of self-interest and will shake the stability of the system must be designed successful p2p systems must be strong against failure

5.2.2 File Poisoning

File poisoning attacks Working on data standards which have become common in p2p networks, the objective of which is to replace a damaged network through another one file and this file does not useless file contaminated Moreover, all messages that pass through it to be poisoned and similar is the a man-in-the-middle attack and given this factors be poisoned Available View high manner which makes them more attractive to download the correct file .

Defenses

Here, the main problem is is that most of the p2p applications be present in the background when you load the contaminated file from a user and be available for a period of time before and be present for a period of time are inspected and eventually is removed all contaminated and the original files become available to all users instead of the damaged .

5.2.3 Sybil Attack

The idea of this attack is to create a fake knot one can form multiple identities on the network and therefore work to gain full control over the network and have already been implementing this plan and an attacker can use a bad protocol in any way possible he can select some of the contaminated files and the striker false identities strategy on the network mode thus, the great damage

Defenses

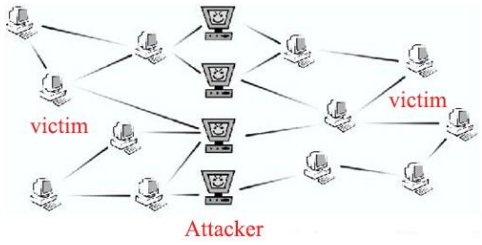
Will speak here about a good defense for the attack, which made an Sybil attack unattractive making it impossible to put malicious identities in strategic locations, we have seen that the network p2p more flexibility and organization to worm propagation and has a good defense mechanism and will be the striker is unable to develop new identities where he pleases and be malicious identities and scattered randomly less serious attacks of strategic and private p2p network that are from large networks

5.2.4 Eclipse Attack

Before the attacker to launch Eclipse attack must be done to control a certain amount of the contract on strategic guidance paths are also network separation into different sub-networks and thus continue the node with another node of the subnet and are at a certain point directing his message through this attack is known (Eclipse) on a subnet and other attacks Eclipse is a measure of the highest-scale man in the middle attacks and attack Eclipse possible to be a continuation of the Sybil attack because the attacker is trying to put a node to him on the strategic direction of the course and as we mentioned earlier that the man in the middle attacks do not pose a significant threat to p2p networks and with Therefore, such an attack be on a large scale and targeting a very serious strategic and be dominant striker on the subnet from the viewpoint of other subsidiary network for display

Defenses

Here are the best solution is the use of randomization algorithm to determine the contract site because it is randomly distributed nodes in a network p2p with no strategy and a striker to control the contract site and it is impossible to separate the two networks subgroups from each other in such conditions



(Fig 7) an Eclipse Attack

6. SECURING P2P NETWORKS

All security issues with p2p networks and mentioned how secure and how to arrange her defenses and how to secure p2p networks through encrypted p2p quartz movement and his peers .

6.1 Encrypting P2P Traffic

Here we will be traffic encryption for network p2p to be encrypted data safely, but more importantly, be careful encryption of the data cannot be easily detected with the original power completely encrypted, it becomes more difficult for the network p2p to be detected for any attack or smothered and be objective is data protection but It has to be simple so that jamming cannot be detected without incurring a lot of fuss and although possible to detect currents Bit Torrent encrypted using sophisticated methods based on the pattern and timing of the traffic but it is much harder to encrypted currents is a p2p traffic encryption seems to be picking up, as currently about 20% of Bit Torrent traffic is encrypted

6.2 Anonymous P2P

By Anonymous peers, Only encryption does not guarantee the protection of users on the network and protect the identity of the decade, while not to reveal his true identity on the network and there is the unknown network p2p who are not trying to detect themselves on the network to find the source or destination data flow They do this by making global network as well as reception also making it difficult to know simply select the data through it is not possible to rely on the use of anonymous p2p sharing application without the use of encryption, however the use of encryption with anonymous p2p result in the experience of using the most secure p2p and available today

7. RESULTS AND FUTURE IMPROVEMENT

We have studied in this research for some of the basics p2p networks, as well as attacks and security issues for these networks, and there President problem to secure p2p networks, a lack of centralized management and thus has no control over the security attacks and is controlled via the p2p through encryption systems unknown and most of these issues aimed IP of the device and to combat these direct attacks on p2p networks must be designed and implemented protocols in the network p2p ..

And also we will talk about the attacks and countermeasures for such joint attacks in the p2p network and we discussed the different categories of p2p systems and analysis of these basic attacks and have some of these attacks, such as the usual online , poisoning attacks and flooding attacks. Others are particular attacks against overlay networks, such as Sybil

attacks and eclipse attacks. The defenses of the attacks are also clarified. For an attack and attack eclipse is they are

actually the most dangerous that threaten network p2p especially network-based overlay attacks on DHT because the attackers take over a large part of the network as well as there are no mature mechanism to stand against them and are providing site of privacy and the site to defend effectively for some of the attacks on the title IP and reduces the chances of such attacks .

We also discussed the means of defense available to some of the attacks, such as Some attacks like SYN flooding and query flooding are easy to launch but can generate effective results. These attacks are prevented by the use of SYN cookies, however you cannot query the flood attack and be p2p structured networks are vulnerable to attack poisoning and can be prone uncle by the attacker because they do not need to add fake addresses to the node table and this attacks can make a large amount and a huge damage to the p2p networks .

Countermeasures to defend each of the general and specific attacks in P2P networks are discussed and analyzed. BitTorrent is used to illustrate the defensive measures against Rational attack and Index Poisoning attack. Examples are used to illustrate various attacks in P2P network. In the following Table 1, we clarify the defense measures and the behaviors of the attacks. Table 1 also summarizes the risk analysis and the level of defense. The summary is derived from the information we collected and analyzed from the above described attacks and defense strategies on P2P networks

Table 1 : the defense measures and the behaviors of the attacks also summarizes the risk analysis and the level of defense

Name of attact	Behavior	Defense strategy	Extent of Danger	Level of Defense
Denial-of-Service (DoS)	1. Flood the network with bogus packets. 2. Drown the victim in fastidious computation.	Pricing	Medium	Easy
Distributed Denial-of-Service (DDoS)	Hacker controls the controlling zombies, through the controlling zombies to control attacking zombies to launch the attack.	Through the trusted server, provide warning system, and created blacklist and white list for trusted visits.	High	Hard
TCP Syn flooding attack	the server gets on TCP Syn on the package and signs of encryption and encryption of some of the security values such as the IP address of the client	when the ACK server receives and is verified ACK before retail is compared with the sequence value,	Medium	Medium
Query Flooding Attack	there are malicious knots are generating inquiries to flood the network as much as possible because if the DDoS query flooding attacks in the central p2p networks	, the victim does not do any response to block traffic but the total amount of inquiries for the attackers may turn out to be a disaster	High	Hard
Man-in-the-middle	An attacker inserts himself undetected between two nodes, and intercept, modify and send data between those two nodes.	Encryption mechanism and authentication technology	Medium	Medium
Worm Propagation	Transits the copies of itself from one node to others automatically.	Firewall, anti-virus and some safety operating system	Medium	Medium
Rational	Download the resource and refuse to upload	Choking algorithm	Medium	Medium
File Poisoning	Poison the index information to make the node hard to find correct content	Authenticate versions and advertisements, rating sources	High	Medium
Sybil	An attack controls a number of identities	Self-Registration algorithm	High	Hard
Eclipse	The malicious nodes work together to fool the good nodes	Indegree and Outdegree method	High	Hard

8. REFERENCES

[1] Prashant Dewan and Partha Dasgupta "P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 22, NO. 7, JULY 2010

[2] Gheorghe, G., Lo Cigno, R., Montresor, A. Security and privacy issues in P2P streaming systems: a survey. Peer-to-Peer Netw. Appl. 4: 75-91, 2011. .

[3] Hyojin Park, Jinhong Yang, Juyoung Park, Shin Gak Kang, Jun Kyun Choi "A Survey on Peer-to-Peer Overlay Network Scheme" Feb. 17-20, 2008 ICACT 2008

[4] J.Schäfer K. Malinka P. Hanáček "Peer-to-Peer Networks Security" IEEE 2008

[5] Xiaowen Yue, Xiaofeng Qiu, Yang Ji, Chunhong Zhang "P2P Attack Taxonomy and relationship Analysis" Feb. 15-18, 20091CACT 2009

[6] Kun, Huang; Lu, Wang, Research of Trust Model Based on Peer-to-Peer Network Security. 2013 International Conference on Information Technology and Applications (ITA), Nov. 2013

[7] Rice, D.O., A Proposal for the Security of Peer-to-Peer (P2P) Networks: a pricing model inspired by the theory of complex networks. 41st Annual Conference on Information Sciences and Systems, 2007. CISS '07., 2007.

[8] Zink, T.; Waldvogel, M., BitTorrent traffic obfuscation: A chase towards semantic traffic identification. 2012 IEEE 12th International Conference on Peer-to-Peer Computing (P2P), pp.126-137, 2012.

[9] Nakamoto, Satoshi, Bitcoin: A peer-to-peer electronic cash system, 2009. 2012. [Online]. Available: http://www.bitcoin.org/ bitcoin.pdf

[10] Chan-Tin, E., Chen, T., Kak, S. A comprehensive security model for networking applications. MobiPST, Munich, July 30- Aug 2, 2012.

[11] Naoum Naoumov and Keith Ross. Exploiting P2P Systems for Dos attacks. Proceeding of the First International Conference on Scalable Information Systems. June – 2006.

[12] Wallach, D.S. (2002) A Survey of Peer-to-Peer Security Issues. International Symposium on Software Security Tokyo, Japan..

[13] Castro, M., Druschel, P., Ganesh, A., Rowstron, A., Wallach, D.S.: Secure routing for structuredpeer-to-peer overlay networks. In: Proc. OSDI 2002, Boston, Massachusetts (2002) To appear.

[14] Sit, E., Morris, R.: Security considerations for peer-to-peer distributed hash tables. In: Proceedings for the 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), Cambridge, Massachusetts (2002)

[15] Riidiger Schollmeier "A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications" IEEE, 2002

[16] Hyojin Park, Jinhong Yang, Juyoung Park, Shin Gak Kang, Jun Kyun Choi "A Survey on Peer-to-Peer Overlay Network Scheme" Feb. 17-20, 2008 ICACT 2008 .

[17] Man Qi "P2P Network-Targeted DDoS Attacks" IEEE 2009

[18] Atul Singh, Miguel Castro, Peter Druschel and Antony Rowstron. Defending Against EclipseAttacks on Overlay Networks ACM. In Proc. of the 11th European SIGOPS Workshop, Leuven, Belgium, September 2004.

[19] Ruichuan Chen, Eng Keong Lua, Jon Crowcroft, Wenjia Guo, Liyong Tang, Zhong Chen "Securing Peer-to-Peer Content Sharing Service from Poisoning Attacks" Eighth International Conference on Peer-to-Peer Computing (P2P'08) IEEE 2008