Security Attacks on Peer-to-Peer Networks

[1]Deepika, [2]Mandeep Kaur
[1]Dept. of ECE, Desh Bhagat Institute of Engg & Management, Moga, Punjab, India
[2]Dept. of Cs/IT, Baring Union Christian College, Batala, Punjab, India

Abstract

In this Paper we try to classify them as well as study the different possible defense mechanisms. In P2P system, which we deeply analyze, including simulating possible behaviors and reactions. Finally, we draw conclusions about what should be avoided when designing P2P applications and give a new possible approach to making a P2P application as resilient as possible to malicious users.

Keywords

Workstation, Proxy Server, Web Server

I. Introduction

In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

The only requirements for a computer to join a peer-to-peer network are an Internet connection and P2P software. Once connected to the network, P2P software allows you to search for files on other people's computers. Meanwhile, other users on the network can search for files on your computer, but typically only within a single folder that you have designated to share.

While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads.

II. Security Goals on Networks

The goals of security mechanism are similar to that of other networks. Security is a great issue in network especially in NETWORKS where security attacks can affect the nodes limited resources and consume them or waste the time before rote chain broke. Security is a vectored term of multi systems, procedures and functions that works together to reach certain level of security attributes.

A. Availability

The main goal of availability is to node will be available to its users when expected, i.e. survivability of network services despite denial of service attack. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network. Again, in higher levels, an adversary could bring down high-level services such as key management service, authentication service .

B. Confidentiality

The goal of confidentiality is to keeping information secret from unauthorized user or nodes. In other words, ensures payload data and header information is never disclosed to unauthorized nodes. The standard approach for keeping information confidential is to encrypt the data with a secret key that only intended receiver's posses, hence achieving confidentiality.

C. Integrity

The goal of integrity is to guarantee the message being transmitted is never corrupted. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways:

1. Malicious Altering

A message can be removed, replayed or revised by an adversary with malicious goal.

2. Accidental Altering

If the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure.

D. Authentication

he goal of authentication is too able to identify a node with which it is communicating and to prevent impersonation. In infrastructure-based wireless network, it is possible to implement a central authority at a point such as base station or access point.

E. Non Repudiation

The main goal of non repudiation is sender of a message cannot deny having sent the message. This is useful when for detection and isolation of compromised nodes. When node P receives an erroneous message from Q, non repudiation allows P to access Q using this message and to convince other nodes that Q is compromised.

F. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users.

III. Attacks on Network

A. Dos Attack

DOS Attacks are the short form for a Denial of Service attack. When you have a DOS attack, it basically means you have had an attack where you have multiple systems being compromised, usually due to being infected with Trojans and these are used to target a single system causing a DOS attack. In a DOS attack, these multiple systems will send a flood of incoming messages that will force the target system to shut down and this will result in a denial of service to the actual or legitimate users. Generally, what happens in a DOS attack is the malicious intruder will look for and exploit a weakness or vulnerability in one computer system and use it as a master system. From the master system, the hacker will then communicate with other systems target to be compromised. The hacker will then load his hacking tools on multiple other systems through the internet. Sometimes, it could be in the thousands of systems that will be compromised. Once done, the hacker will be able to easily instruct the compromised systems to launch attacks against a specified target causing a denial of service here.

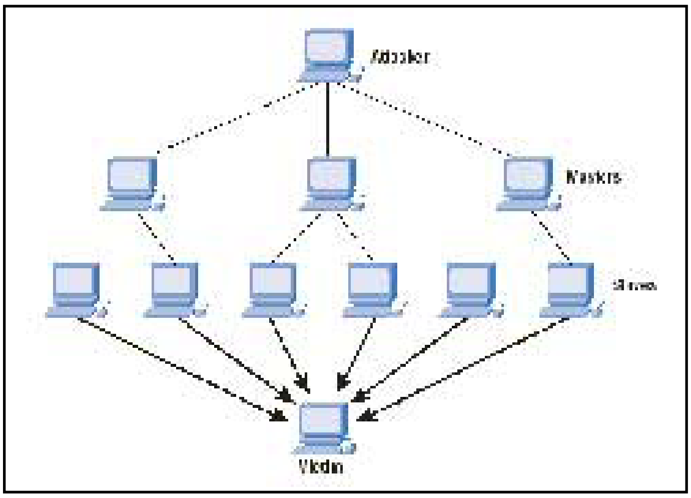

Fig. 1: Dos Attack

The systems that have been controlled by the hacker are called zombies or bots. These can be numerous in number and will function as an army for the hacker to achieve his aim of attacking his target.

B. Man in the Middle Attack

The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in figure 1.2. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.

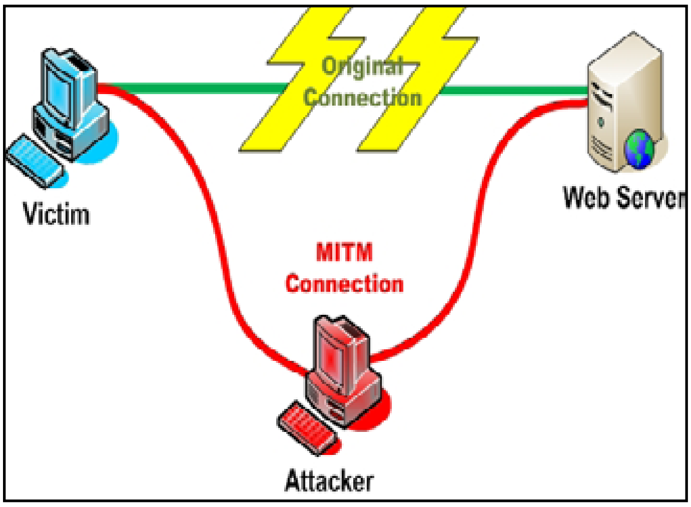

Fig. 2: Man in the Middle Attack

C. Sybil Attack

Malicious nodes in a network may not only impersonate one node, they could asume the identity of several nodes, by doing so undermining(destroy) the redundancy(repeating) of many routing protocols. This attack is called the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for storage, routing mechanism, air resource allocation and misbehavior detection. Basically, any peer-to-peer network (especially wireless adhoc networks) is vulnerable to Sybil attack.

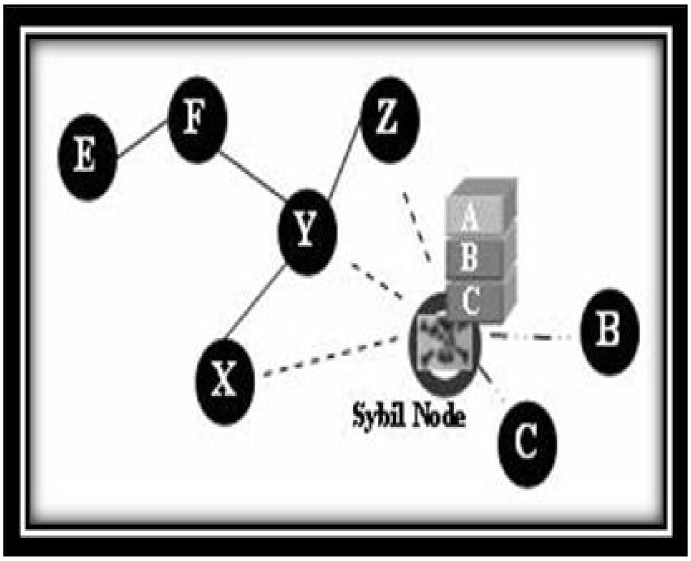

Fig. 3: Sybil Attack

D. Tunneling Attack

Tunneling attack is also called wormhole attack. In a tunneling attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers.

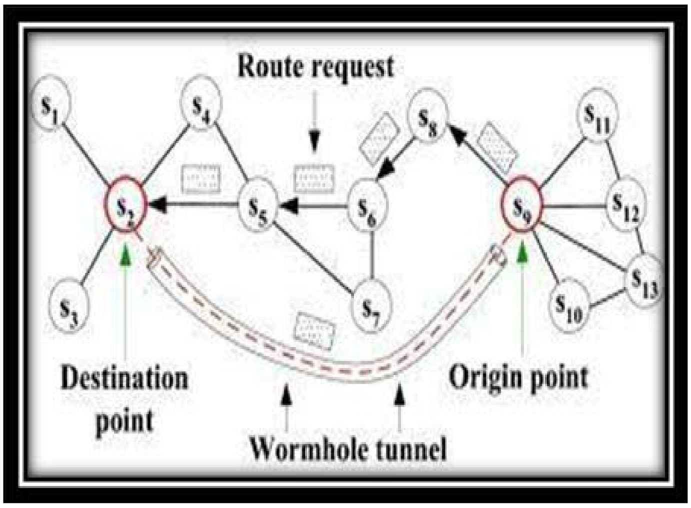

Fig. 4: Tunneling Attack

E. Eclipse Attack

Before an attacker can launch an eclipse attack, he must gain control over a certain amount of nodes along strategic routing paths. Once he has achieved this, he can then separate the network in different subnetworks. Thus, if a node wants to communicate with a node from the other subnetwork, his message must at a certain point be routed through one of the attacker's nodes. The attacker thus "eclipses" each subnetwork from the other. In a way, eclipse attacks are high-scale man-in-the-middle attacks. An Eclipse attack can be the continuation of a Sybil attack. In this case, the attacker will try to place his nodes on the strategic routing paths. We argued before, that man-in-the-middle attacks don't pose a great threat to P2P networks. However, such a high scale attack involving strategic targeting is very serious. The attacker can completely control a subnetwork from the other subnetwork's point of view. If an attacker manages an Eclipse attack (it is not an easy attack), can attack the network in a much more efficient manner.

- He can attack the control plane by inefficiently rerouting each message.
- He can decide to drop all messages he receives, thus completely separating both subnetworks.
- He can attack the data plane by injecting polluted files or requesting polluted files on behalf of a innocent nodes and hoping, these files are cached or copied along the way.

F. Rational Attacks

Peer to Peer services to be effective, participating nodes must cooperate, but in most scenarios a node represents a self-interested party and cooperation can neither be expected nor enforced. A reasonable assumption is that a large fraction of P2P nodes are rational and will attempt to maximize their consumption of system resources while minimizing the use of their own. For example nodes might realize that by not sharing, they save precious upload bandwidth. In the case of copyrighted material, file sharing can have worst .As it is illegal and quite easy for authorities to find out who is sharing specific files, it can lead to a very big fine. These are good enough reasons to motivate nodes in becoming “self-interested”. If a large number of nodes are self-interested and refuse to contribute, the system may destabilize. Successful P2P systems must be designed to be robust against this class of failure.

G. File Poisoning

File poisoning attacks operate on the data plane and have become extremely commonplace in P2P networks. The goal of this attack is to replace a file in the network by a false one. This polluted file is of course of no use. t has been reported, that the music industry have massively released false content on P2P networks. Moreover, companies such as Overpeer1 or Retsnap publicly offer their pollution-based services to the entertainment industry as a way for protecting copyrighted materials. In order to attack by file poisoning, malicious nodes will falsely claim owning a file, and upon a request will answer with a corrupt file. For a certain amount of money, Overpeer or Retsnap will release huge amounts of fake copies of a file on their servers. Moreover, all messages passing through malicious node can be poisoned (similar to a man-in-the-middle attack). These factors may give the poisoned file a high availability, making it more attractive to download the true file.

IV. Simulation

Freenet is an enhanced open source implementation of the system described by Ian Clarke’s and is classified as a third generation P2P application. A first version was released in March 2000. Freenet was designed to answer privacy and availability problems second generation applications currently experience. It was built in order to achieve following 5 requirements:

- Anonymity for both producers and consumers of information.
- Deniability for storers of information.
- Resistance to attempts of third parties to deny access to information.
- Efficient dynamic storage and routing of information.
- Decentralization of all network functions.

Intuitively, Freenet can be seen as a “chained” network. Like a link in a chain, each node can only communicate with its direct neighbors. When a node wants to query a file, it sends the message to the most promising neighbor, which will in turn also forward it to its most promising neighbor. Once a message is sent, a node has no way of finding out what will happen to it. It cannot tell to which node the neighbor will in turn forward the message to, or even whether the message is directly answered by the neighbor itself. What’s more, a node receiving a message cannot tell if this message originates from this neighbor or if it is merely forwarding a message received by a previous neighbor.

In order to have a precise idea of which attacks are most efficient against the Freenet structure, we decided to write a simulation of the Freenet network. The nodes’ behavior was programmed in order to be as close to a normal Freenet node as possible. They have limited storage space (40 files maximum), can only connect to a limited number of neighbors and can disconnect from the network during the simulation run. Each node receives at the beginning several files (15 in this case) selected randomly from a global library containing 10000 different files who’s keys were uniformly distributed. What’s more, there is no pre-network structure. Each node inserts himself in the network at a random node and then proceeds to query random files. The network is thus dynamically built during the first 5000 random queries of each run of the simulation, an initialization phase we do not consider for the results. The simulation is then tested for an additional 1000 rounds during which all results are monitored. Messages were given a TTL of 20 hops and could be corrupted by malicious nodes. The simulation was run several times with 2000 good nodes and 20 malicious nodes, the malicious nodes pretending to be good during the initialization phase. Before discussing the results, we would like to underline the fact that simulations can never perfectly model reality however precisely they were implemented. We will therefore not use the results directly but more to get an idea of which attacks would be most effective. Even though, the simulation proved remarkably robust against variable changes (changing the TTLs, the storage space ...) which only mildly affected the final result.

V. RESULTS

The first runs of the simulation were done with only good nodes. The simulation returned an average of 90% successes which is quite plausible. Indeed, it is possible that a node chooses to query data which is not available on the network. The other failures are due to the TTL which expired before the file was reached.

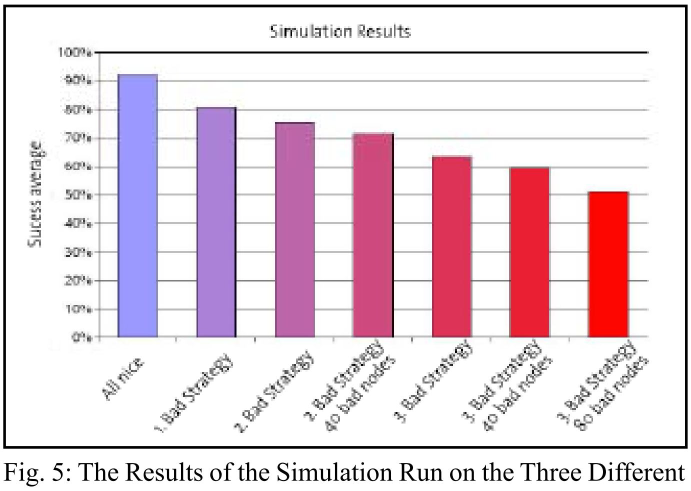

Fig. 5: The Results of the Simulation Run on the Three Different Malicious Strategies

We then tried out the first attack: all bad nodes should forward each message to the worst possible node instead of the most qualified.

This barely had an impact, the simulation showed an average of about 80% successes. This is understandable as forwarding the message to the least qualified node is equivalent to starting a query with a diminished TTL.

The second attack simulated was to make malicious nodes overwrite every data source with the worst possible data-source. The results were comparable to the first malicious strategy, although a little more effective. The simulator indicated an average success rate of 73%. This success rate barely changed when we doubled, then trippled the number of malicious nodes.

Finally, we tried the last attack: all bad nodes should corrupt each message which passes through them. This time, the simulation showed only 63% success. We then decided to double the number of malicious nodes making them 40. With only 40 malicious nodes and 2000 good nodes, the simulation then showed an average success of only 56%. It came down to a 51% success average when we doubled the number of malicious nodes again.

VI. Conclusion

The simulation clearly shows Freenet is capable to adapt to the first two attacks. Its model is flexible enough to defeat both attacks which aimed to destroy the nodes' specialization. Yet it is very vulnerable to the third kind of attack as 2% malicious nodes can already reduce the success rate to nearly 50%. We have now finished our analysis of security in P2P networks. As a conclusion we can re-express the fact that only pure P2P stand a chance against attacks, any kind of shortcuts taken in the implementation can be turned around in order to attack the P2P application in a more dangerous manner. We finally observed that it would be interesting for a PGP-like application to exist. This application should not solely worry about authenticating users but also how much trust can be given to a public key. If such an application existed, it could be used by P2P applications as a very efficient protection against malicious attacks.

Reference

[1] Dr.Gurjeet Singh,"Performance and Effectiveness of Secure Routing Protocols in MANET", Global Journal of Computer Science & Technology, Vol. 12, Issue 5, 2012.

[2] Dr.Gurjeet Singh, Dr. Jatinder Singh,"Security Issues in Broadband Wireless Networks", Global Journal of Researches in Engineering Electrical and Electronics Engineering, Vol. 12, Issue 5, 2012.

[3] Pierre Trudeau (2001),"Building Secure Wireless Local Area Networks", White Papers at Colubris.com, [Online] Available:http://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf

[4] Lidong Zhou, Lintao Zhang, Frank McSherry, Nicole Immorlica, Manuel Costa, Steve Chien,"A First Look at Peer-to-Peer Worms: Threats and Defenses", Vol. 10, Issue 4, 2012.

[5] WLAN Association (1999),"Introduction to Wireless LANs", WLAN A Resource Center, [Online] Available: http://www.wlana.com/learn/intro.pdf

[6] John Vollbrecht, David Rago, Robert Moskowitz (2001),"Wireless LAN Access Control and Authentication", White Papers at Interlink Networks Resource Library, [Online] Available] http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf

[7] WLAN Association (2002),"Wireless Networking Standards and Organizations", WLANA Resource Center, [Online] Available] http://www.wlana.com/pdf/wlan_standards_orgs.pdf

[8] Interlink Networks (2002),"Wireless LAN Security using Interlink Networks RAD Series AAA Server and Cisco EAP-LEAP", Application Notes at Interlink Networks Resource Library, [Online] Available] http://interlinknetworks.com/images/resource/wireless_lan_security.pdf.

[9] Jesse R.Walker (2000),"Unsafe at any key size; An analysis of the WEP encapsulation", 802.11 Security Papers at NetSys.com. [Online] Available] http://www.netsys.com/library/papers/walker-2000-10-27.pdf