Security Risk Analysis in Peer 2 Peer System; An Approach towards Surmounting Security Challenges

Mansoor Ebrahim, Shujaat Khan, and Umer Bin Khalid

Abstract—P2P networking has become a promising technology and has achieved popularity as a mechanism for users to share files without the need for centralized servers. The rapid growth of P2P networks beginning with Kazza, Lime wire, Napsters, E-donkey, Gnutella etc makes them an attractive target to the creators of viruses and other security threats. This paper describes the major security issues on P2P networks (Viruses and worms) and presents the study of propagation mechanisms. In particular, the paper explores different P2P viruses and worms, their propagation methodology, outlines the challenges, and evaluates how P2P worms affect the network. The experimental results obtained will provide new direction in surmounting the security concerns in P2P Networks.

Index Terms — P2P, Viruses, Worms, Simulators, Propagation.

I. INTRODUCTION

P2P is a wide and significant field for research and is the expected consequence of the Internet and business-related efforts to interconnect computer systems for competent sharing of information. P2P has enormous potential in distributed computing, as large networks such as the Internet, when merged different types of information sharing technologies, enables computing to occur on a distributed basis [19]. P2P technologies are trickling into the largest corporations and business organizations in the form of distributed-computing services and becoming a significant part of industries.

The emergent popularity and infiltration of P2P networks has made them a prospective medium to the creators of viruses and other security threats by providing them with effective means of compromising hosts on a large scale. Worms are special type of viruses that replicates itself and spreads without user interaction. Similarly, the high risks involved in P2P systems have focused attention on various security issues like Confidentiality, Authentication, Interoperability, Vulnerability, and Integrity in the P2P network environment [1]. The study P2P systems comprise on the standard of network simulation first and then experimentation in the real environment. Simulations are the most prevailing and distinguished elements for analyzing and scrutinizing different type of networks and P2P applications. The simulations can be performed with low cost as compared to large-scale experiment [17].

The rest of the paper is organized as follows. Section II intricate on the upcoming threat of P2P worms and defining new defence mechanisms. Section III describes a model of virus propagation in a P2P network. The evaluation of different types of existing P2P simulators as well as a survey and comparison of existing P2P simulators with selection of the best simulator among them appears in Section IV. We conclude in Section V.

II. SECURITY CONCERNS

This section discuss the security issues occurs in a pure P2P network posed by P2P worms as well as also describes different known viruses in a P2P network and gives a high level description of the ones that are most threatening.

Viruses and worms are the major security threats attacking the business environment infrastructure. In P2P applications, security of files & directories are the accountability of individual users. Thus P2P applications are more exposed to security concerns and counter act measures should be taken to defend perceptive and copyright protected information within the system.

The P2P security issues can be classified upon different service provisions parameters. In General, the security of P2P systems should involve four main service areas that includes distributed computing, file sharing, collaboration, platforms and these services are simply comprehended when in view of exclusive characteristics of P2P systems [1]. Recently a number of viruses are designed that exclusively spread via P2P networks. Swen, Fizzer, Lirva A, Lirva B, Mandragore, Benjamin A-B, Lolola, & Magic Eight Ball etc are prominent P2P viruses that have emerged rapidly as shown in figure 1.

Mansoor Ebrahim is Assistant Professor at Iqra University, Defence View campus, Karachi, Pakistan (phone: 0092-331-2543-160; e-mail: mebrahim@iqra.edu.pk).
Shujaat Khan is Lecturer at Iqra University, Defence View campus, Karachi, Pakistan (e-mail: shujaat@iqra.edu.pk).
Umer Bin Khalid is engineering student at Iqra University, Defence View campus, Karachi, Pakistan (e-mail: umerkhalid456@gmail.com).

Figure 1: Most Prominent P2P Network Viruses
A. Swen Virus
1) Introduction
I-Worm.Swen [2] also called, as Gibe.2 is one of the famous P2P viruses that mainly affect P2P networks such as Kazaa, Gnutella. It is a malicious program mainly broadcast through email, instant messaging, and Internet chat rooms.

2) Propagation Methodology
It propagates through email, Instant Messaging (IM), Internet chat room through P2P applications by making multiple copies of itself and placing them in the shared folder chosen from a list of file names generally comes in a hidden form of Microsoft Patch Mails itself to email addresses selected from the victim’s email address book and sent folders it also introduces false errors in Windows Messaging API (MAPI) and asks users for confidential information such as password, SMTP server, account, etc. [2].

3) Aliases
Its aliases are Swen [F-Secure], W32/Swen@mm [McAfee], W32/Gibe-F [Sophos], I-Worm.Swen [KAV], Win32 Swen.A [CA], WORM_SWEN.A [Trend] [2].

4) Virus Outline

| Type               | Untamed Level | Infection Nodes | Number of Sites | Geological Distribution | Threat Restraint | Removal | Damage Intensity | Distribution Intensity | Written By |
|--------------------|---------------|-----------------|-----------------|-------------------------|------------------|---------|------------------|------------------------|------------|
| Type               | Low           | above 1000      | above 10        | High                    | Easy             | Difficult | Medium          | High                   | John Canavan |

B. Fizzer Worm
1) Introduction
Fizzer [2] worm also known as Win32/Fizzer.A@mm is similar to Swen virus and is also one of the most popular viruses in P2P networks.

2) Propagation Methodology
It Propagation methodology is similar to Swen virus i.e. through email, Instant Messaging (IM), Internet chat rooms through P2P applications by making multiple copies of itself and placing them in the shared folder chosen from a list of filenames, it contains backdoor and key logger abilities. Backdoor component allows virus to issue commands on victim’s computer uses mIRC and AOL Instant Messenger (AIM). Key logger stores data being input by the victim and hence allowing the virus author to view confidential data such as password, account details, etc. Attempts to shutdown anti-virus programs [2].

3) Aliases
Its aliases are W32/Fizzer@MM [McAfee], Win32.Fizzer [CA], W32/Fizzer-A [Sophos], WORM_FIZZER.A [Trend], Fizzer [F-Secure], Win32/Fizzer.A@mm [RAV], I-Worm.Fizzer [KAV] [2].

4) Virus Outline

| Type               | Untamed Level | Infection Nodes | Number of Sites | Geological Distribution | Threat Restraint | Removal | Damage Intensity | Distribution Intensity | Written By |
|--------------------|---------------|-----------------|-----------------|-------------------------|------------------|---------|------------------|------------------------|------------|
| Type               | Low           | 0 - 49          | 0 - 2           | Low                     | Easy             | Easy    | Low              | Medium                 | Neal Hindocha |

C. Mandragore
1) Introduction
Mandragore [2] is a worm that infects and spreads through Gnutella type P2P networks that are based on Win32 systems. It is an application of 8192 bytes in length.

2) Propagation Methodology
It propagates upon infection, registers itself as a Gnutella network node, listens to traffic of file requests and reply positively to corresponding requests, it reports the file name being searched with ".exe" extension, it gets activated when the victim runs the infected file. Worm thread performs two actions: it tries to pretend as Gnutella node, and shows the fake file the user was looking for. The filename has an ".exe" extension, and with worm code in it [2].

3) Aliases
Its aliases are W32.Gnutella, Gnutella Mandragore, and W32.Gspot.Worm [2]

4) Virus Outline

| Type               | Untamed Level | Infection Nodes | Number of Sites | Geological Distribution | Threat Restraint | Removal | Damage Intensity | Distribution Intensity | Written By |
|--------------------|---------------|-----------------|-----------------|-------------------------|------------------|---------|------------------|------------------------|------------|
| Type               | Low           | 0 - 49          | 0 - 2           | Low                     | Easy             | Easy    | Low              | Medium                 | Neal Hindocha |

D. Lirva A and Lirva B
1) Introduction
Lirva A and Lirva B [2] viruses mostly affect kazaa P2P networks. These viruses are much dangerous as compared to the ones mentioned above. It attempts to shutdown firewall and anti-virus applications, scans Outlook address books and mail itself on addresses in the sent folder.
2) Propagation Methodology
Virus can be spread through the following files: Resume.exe, Download.exe, MSO-Patch-0071.exe, MSO-Patch-0035.exe, Two-Up-Secretly.exe, Readme.exe, Singles.exe, Sophos.exe, Cogito_Ergo_Sum.exe, and IAmWithYou.exe [2].

3) Aliases
Its aliases are, W32/Avril-A [Sophos], W32/Lirva.b@MM [McAfee], WORM_LIRVA.A [Trend], Win32.Lirva.A [CA], I-Worm.Avron.c [KAV], Lirva [F-Secure] [2].

4) Virus Outline

| Table 3: Summary of Lirva Virus |
|--------------------------------|
| **Type**       | Wild worm     |
| **Untamed Level** | Medium        |
| **Infection Nodes** | above 1000   |
| **Number of Sites** | above 10     |
| **Geological Distribution** | High         |
| **Threat Restraint** | Easy          |
| **Removal**      | Moderate      |
| **Damage Intensity** | Medium       |
| **Distribution Intensity** | High         |
| **Written By**  | Atli Gudmundsson |

E. Benjamin.A and Benjamin.B
1) Introduction
The Benjamin [3] worms are a strong security threat to P2P networks. These worms are occasionally found to attack Kazaa networks without their authorization or awareness [4].

2) Propagation Methodology
It displays some fake error messages such as “Access error #03A. 94574: Invalid pointer operation File possibly corrupted.” Once Worms then creates hundreds of copies of its files and places them in the shared folder of all the users in the network [4].

3) Aliases
Its aliases are Worm.P2P.Benjamin.a, W32/Lirva.A [CA], I-Worm.Avron.c [KAV], Lirva [F-Secure] [2].

4) Virus Outline

| Table 5: Summary of Benjamin Virus |
|-----------------------------------|
| **Type**       | Wild worm     |
| **Untamed Level** | Medium        |
| **Geological Distribution** | Low          |
| **Threat Restraint** | Moderate     |
| **Removal**      | Moderate      |
| **Damage Intensity** | High         |
| **Distribution Intensity** | Low          |

F. Lolol.a
1) Introduction
Lolol [18] is another worm that spreads rapidly in a P2P network. This worm is similar to fizzer worm in behaviour and has reported to infect many Kazaa file-sharing networks. [4].

2) Propagation Methodology
It consists of a powerful backdoor routine that connects to IRC channel where it executes commands send by the author of the worm. It is a 60 KB Windows PE.exe file and written in Microsoft Visual C++ [4].

3) Aliases
Its aliases are Worm.P2P.Lolol.am, W32/Lolol.worm.gen, Win32.HLLW.Lolol.58400, W32/Lolol.A [Sophos], Win32/HL LW.Lolol.A [RAV], WORM_LOLOL.A [Trend Micro], and Worm/Lolol.gen [H+ BEDV], and Win32: Trojan-gen. [ALWIL] [5].

4) Virus Outline

| Table 6: Summary of Lolol.a Virus |
|-----------------------------------|
| **Type**       | Wild worm     |
| **Untamed Level** | Low           |
| **Geological Distribution** | Low          |
| **Threat Restraint** | Moderate     |
| **Removal**      | Easy          |
| **Damage Intensity** | Medium       |
| **Distribution Intensity** | High         |
| **Written By**  | David Perry   |

G. Magic Eight ball
1) Introduction
Magic Eight ball [3] is known to be a Trojan virus that infects P2P networks such as Kazaa. Magic Eight ball comes in a packaged Zip file known as eightball2.zip [4].

2) Propagation Methodology
Its Attempts to delete files on C: directory, once executed, Trojan creates a batch file that contains instructions to delete files from the root directory. It displays a series of dialogue boxes and when OK is pressed on the last dialogue box then the virus activates [4].

H. Comparison of Viruses on Security Parameters:
Figure 2 depicts the overall comparison of the above analysed P2P network viruses. The viruses were evaluated on the bases of following security parameters:

- Damage Level
- Distribution Level
- Removal Difficulties
- Threat Containment
- Geographical Distribution
- Number Of Source Sites
- Number Of Infections
- Wild Level
III. VIRUS PROPAGATION MODELING

In this section the model of a virus (Swen) is designed and its propagation process through epidemiological models is examined. The Mathematical Epidemiology is credited to McKendrick and his seminal; epidemiology is the field of biology which deals with the modelling of diseases spreading in a population [14]. Epidemiological modelling has been used in previous studies and designing computer virus and worm.

A. Epidemiological Modelling schemes

The Epidemiological modelling of computer viruses mainly makes use of either the susceptible-infected-susceptible (SIS) model or the susceptible-infected-removed (SIR) model even though there is another model called as susceptible-infected-exposed-removed (SIER).

SIS model, each host stays in one of two states: susceptible or infectious. Each susceptible host becomes an infectious one at a certain rate. At the same time, infectious hosts are cured and become again susceptible at a different rate. This model system where having the infection and being cured does not confer immunity.

SIR model, a node cannot be infected more than once [6].

SIER model, a node cannot be infected more than once which cause an individual to be able to infect others immediately upon their infection. Many viruses have what is termed a latent or exposed phase, during which the individual is said to be infected but not infectious.

B. Related Work

This section discusses brief overview of work related to virus propagation in P2P networks. More recently, several authors have utilized epidemiological models to study the spread of worms [11] and e-mail viruses in the Internet [12]. There have been a number of recent papers [6, 7, 8, 9, 13 and 14] which model virus and file propagation in P2P networks.

In [7], a model of infected file propagation in P2P networks is examined. The file propagation model is based on basic epidemiological model i.e. S-E-I (Susceptible-Exposed-Infected) model. The file propagation model make user of some discrete equations used to detect the behaviour of peers depending on the three states along time and finally reach a steady state. The model analysis is based on numerical calculations and assumptions. Such analysis cannot be proved to be 100% correct unless performed on a P2P network simulator.

The research paper in [6] is the modified version of the work mentioned in [7] by the same group of people. In this paper, the additional work includes the study of dissemination of polluted files and the release of P2P viruses. Extension in modelling includes the modelling of Online/Offline behaviour of peers and the modelling of peers that remain infected and their corresponding equations.

In [8], is related to the above-discussed approaches for modelling virus propagation in Gnutella P2P networks. In this paper, the authors have formulated an analytical model that gives light to mechanics of a decentralised Gnutella type P2P network and virus propagation in such networks.

The research paper in [9] presents the threats caused by P2P worms and possible mechanisms to avoid such threats. The proposed defence mechanism consists of guardian nodes that automatically detects worms and sends alert messages to other peers in the network. They formed a basic model in order to perform virus propagation and presented a theoretical analysis. The theoretical analyses are also supported by experiments.
performed on P2P graphs generated by a P2P simulator but the name of the simulator is not mentioned.

The examination of the behaviour of viruses in P2P networks is discussed in [14]. This paper contributes to propose a model of virus propagation, which can be used to predict virus behaviours.

In [13], a method is proposed on the propagation of active worms in P2P networks. The analysis on simulation results shows that there exists some threshold value during dispersal of worms and different infection schemes result in different infection results in P2P networks.

C. C. Virus Model

1) Model Description

The intent of the model is to predict the expected behaviour of a virus as well as to monitor the effect of the virus which spreads through a P2P network in the form of malicious code embedded in executable files shared by peers [16].

The research paper [16] presents details of the above mentioned Virus Model based on epidemic model. The paper predicts how a virus propagates in a P2P network as well as address issues related to virus propagation in a P2P network. The paper includes assumptions, parameters, equations and evaluation of virus propagation, representation and implementation of virus mathematical model exclusively Swen virus in Gnutella network and analyzing its performance.

D. Simulator Analysis

Simulations are the most prevailing and prominent tool for evaluating and exploring different type of P2P networks and applications [17].

The study of P2P systems comprise on the standard of network simulation first and then experimentation in the real environment. However during the simulator research it was found that not only are there different simulators in use, but the simulators that are accessible did not have the ability to generate significant data for analysis. A lack of standard documentation makes verification of results harder as well as due to such poor documentation implementation of well-known overlay algorithms was very difficult [10].

The figure 5 summarizes and analyses the general aspects of all the simulators and on the basis of these analyses a simulator Peer Thing was selected that most satisfies the simulation requirement in order to model virus propagation in P2P networks.

In [17] analytical review regarding major P2P simulators is carried out. The Paper describes different types of existing P2P simulators as well as provides a survey and comparison of existing P2P simulators and extracting the best simulator among them.
PeerThing is very easy to handle and use, as there is no need to install the PeerThing simulator as the PeerThing developer has made an executable file of the simulator, execute the .exe file and the simulator starts. PeerThing is a graphical based simulator that made it easy to use. The user has to perform three basic steps to perform any simulation. The basic steps consist of defining system behaviour then creating a scenario and finally defining a query to view the simulation results. PeerThing has the capability of storing the generated results to be viewed later. The generated results can be transformed into .csv format that can be visualised in MS Excel for further analysis. The simulator contains a detailed user manual to assist its users to perform simulations. Its online support is also available through group mails since it is currently in active state [17].

Gnutella Experimental Setup Simulation

1) Gnutella Model

In this section, the experimental setup of Gnutella model in Peer Thing simulator is presented. Figure 6 and 7 shows the representation of Gnutella model and implementation of Swen virus in it respectively, Gnutella is a pure P2P architecture; therefore it consists of servants that act as both, as peers and servers. The behaviour of peers and servers are defined in the System Behaviour Editor and the scenario associated with the architecture is defined in the Scenario Editor.

2) Implementation of Swen in Gnutella Network

In [16] detailed description of System Behaviour and Scenario for Gnutella simulation setup is mentioned, the Swen virus is modelled in Gnutella network and its performance analyses is carried out.

IV. EVALUATIONS AND RESULTS

In this section several simulations have been performed to analyse the basic behaviour of a Gnutella network and propagation of virus in a Gnutella network. The research paper [17] presents details of the simulation results obtained from simulator runs with the Gnutella protocol, different analysis extracted on the basis of obtained simulation results.

1) Number of Downloads In Gnutella Network

As there is an increase in the size of P2P network, the no of files searched and found increases [16].
2) The Sensitivity of P2P System Size
As there is an increase in the size of P2P network, the attack performance becomes constantly better for all attack tactics [16].

3) Re-infection V/s Non re-infection
In Re-infection virus propagates faster than Non-Re-infection.

4) The sensitivity of P2P vulnerability
As there is an increase susceptibility of P2P peers, the attack performance becomes constantly better for all attack tactics [16].

5) Overall System Analysis
How the number of peers falling into each of the three categories susceptible, exposed and infected evolves over time [16].
[11] J. R. Crandall and F. T. Chong. Minos: Control data attack prevention orthogonal to memory model. In Proceedings of the 37th Annual IEEE/ACM International Symposium on Microarchitecture. IEEE/ACM, December 2004.

[12] J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan. Fast portscan detection using sequential hypothesis testing. In Proc. 25th Symposium on Security and Privacy. IEEE.

[13] Laurence Cuthbet, Laurissa Tokarchuk, “Propagation Model of Active Worms in P2P Networks Department of the Electronic Engineering”, Queen Mary, University of London, UK.

[14] Chao-Sheng Feng, Zhu-Guang Qin, Laurence Cuthbet, Laurissa Tokarchuk, “Propagation Modeling And Analysis Of Viruses In P2p Networks”

[15] Funda Samanioglua, Ayse Humeyra Bilgeb, Onur Ergonuk, A Susceptible-Exposed-Infected-Removed (Seir) Model, Department of Industrial Engineering, Kadir Has University, Istanbul, TURKEY.

[16] Mansoor Ebrahim, Syed Umar Talha, Jahanzeb Ahmad, Modeling Virus Propagation in Pure Peer-to-Peer Networks, FIT ‘10 Proceedings of the 8th International Conference on Frontiers of Information Technology.

[17] Mansoor Ebrahim, Shujaat Khan and Syed Sheraz Ul Hasan Mohani, Peer-to-Peer Network Simulators: an Analytical Review, Asian Journal of Engineering Science and Technology AJEST Volume No 2 Issue 1 2012, Karachi Pakistan.

[18] Choon Hoong Ding, Sarana Nutanong, and Rajkumar Buyya, writers, (2002-03), Peer-to-Peer Networks for Content Sharing.

[19] Richard Thommes and Mark Coates,(2006), Epidemiological Modelling of Peer-to-Peer Viruses and Pollution, Department of Electrical and Computer Engineering, McGill University, Canada.