

Digital Privacy and Security: A Survey on the Modern Threat on the Digitization

Soumee Maschatak^{1*}, Chandan Raj BR²

^{1,2}Dept. of Computer Science and Engineering, East West Institute of Technology, VTU, Bangalore, India,

DOI: <https://doi.org/10.26438/ijcse/v7si15.339343> | Available online at: www.ijcseonline.org

Abstract – Today’s software industry is operating on losses because of a modern threat known as Digital Piracy. Not only the software industry, various sectors of the industry like the cinematography, authors, inventors and discoverers are facing a threat wherein their work may attain a global attention without bringing them anything. A recent studies has shown that due to recent craze of digitization and the socio-economic condition, people are more inclined towards acquiring everything without even giving it time and money. This is becoming a threat to the intellectual property owners. This paper is all about understanding the factors affecting digital piracy, the types of digital piracy and the various steps and measures needed to stop the digital piracy from spreading its wings.

Keywords – Piracy, factors, types, peer-to-peer applications, BitTorrent

I. INTRODUCTION

With the advent of 21st century, the world has seen an increase in the number of the people using the internet. People has moved online for their day-to-day necessities. In an article on Internet and public policy, Margetts (2009) has presented data showing that ‘for many people across the world, large chunks of their social, economic and political life have moved online’. With such a huge number of people being addicted to the online life, the number of criminal activities associated with it has also increased to a great extent, which is popularly known as *digital piracy*.

Digital piracy refers to the unauthorized, prohibited and unlicensed use/ downloading of copyrighted software, digital videos, and digital documents for using it for one’s own individual profit or for an organization. Digital piracy mostly happens over social media or via the internet. It is a felony offense, because once it is available over the internet, it gets very difficult to stop the spreading of the videos or the software. Even if one removes the pirated contents from the internet, one may never know if someone else have already downloaded the contents and spreading it offline. Hence it becomes increasingly important to safeguard the licenses and the authority of such contents and that’s where security comes into play. Many national and international laws have been made and implemented to prevent such acts of piracy.

This article is based on a detailed description on how and why digital piracy has become a global concern and what should be the necessary steps to prevent it from spreading. Our goal is to throw some light on the urgency on the concern raised and also come up with some solutions which

could be practised at an individual level to prevent digital piracy.

II. RELATED WORK

This section provides an insight into the work that has already been contributed in the field of digital piracy prevention and security.

Factors affecting digital piracy

Software companies are facing acute losses due to software piracy which instigates them to come up with some technical measures to prevent the piracy. The first thing is to identify the factors that promotes digital piracy. Many experiences have been performed to find out the exact reasons and the factors that are involved in spreading digital piracy. Factors like *age, gender, financial status, moral judgement, cognitive beliefs and subjective norms* play a very big role in spreading digital piracy. We will throw some light on each of these points.

Age – There exist a large body of ethics literature that is concerned with individual attributes and their effect on decision making. Studies suggest that older people tends to have higher ethical values than the younger generation. Hence, the older generation feels it to be unethical to be involve themselves with digital piracy. Therefore, we can conclude that people of young generation, mostly around the age of 15 to 35 are involved in promoting digital piracy.

Gender – Gender has been found to be one of the variable factor affecting digital piracy. The ethics literature establishes the fact that the females have a higher ethical

standards than the males (Ford and Richardson, 1994). Sims et al (1996) found out that the males have a higher tendency to pirate the software than the females. With regards to the ethics literature, hence, we can say that female gender has a lower attitude to digital piracy than the males.

Financial Status – The commercial status of the society also plays a vital role in determining the factor of digital piracy. Studies have revealed that the students, generally the college going students have a tendency to download the software and the movies as they do not have the requisite means to afford them. Hence affordability becomes a factor in spreading digital piracy. People with a proper economic means prefer to own the movie tickets or the software licenses. Hence, it can be concluded that people with lower economic means adds up to the spreading of digital piracy.

Moral judgement –Moral judgement is used to define the way a person reaches his/her decision when faced with a dilemma (Kohlberg, 1969). According to Kohlberg, individuals with high moral judgement think of the society and other people surrounding them before reaching a conclusion. Hence, people with high moral judgement tends to indulge themselves less in digital piracy.

Cognitive beliefs –Cognitive beliefs refers to the mental system of an individual consisting of interrelated items of assumptions, ideas, beliefs, ideas and knowledge that an individual holds about anything concrete or abstract. A detailed and a more recent approach has encouraged that an individual's attitude is not only based on the cognitive beliefs but also on the feelings and emotion towards performing the behaviour or the object, also known as affective beliefs. Studies claim that people who score high on the excitement and happiness scale will have a greater attraction to indulge themselves in digital privacy than the people who are ranked high on depression scale.

Subjective norms –Subjective norm is perceived as the social pressure to engage or not to engage in a behaviour. Subjective norms are theorized to influence attitude. The higher the evaluation of subjective norms (significant others have a favourable opinion towards the behaviour), the higher attitude towards digital piracy.

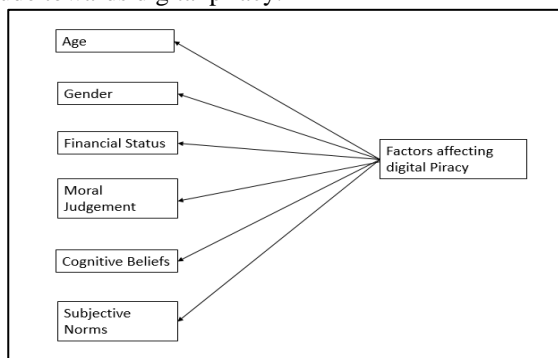


Fig. 1: Factors affecting Digital Piracy

Types of digital piracy

One's online life may not seem worth tracking as a common man can browse only through the websites to get some information or be uploading and be an active member in the social media. But when we look at the bigger picture, which people often fails to see, is that people often generates rich trove of information about that person, which if analysed properly can depict the type of person you are and what are your areas of interest. This collection of information for data analyse is totally invisible to the users. This is actually a tempting area for marketers and law enforcement officials.

There are five main types of digital piracy. They are –

Cookie proliferation –A cookie is a text file which the web browser stores on the user's machine. It gets destroyed as soon as the user closes the web browser. The text file stores contents such as authentication information, storing website information, other browsing information and anything else that can help the web browsers while accessing web servers. The invisible cookie software agents tracks down the browsing habits and collects personal data. Advertising networks, marketers, data analysers can collect more information this way and then store them with themselves. They can later retrieve these information and analyse it to generate a pattern of your browsing.

These has increased manifold now-a-days. Big companies have even crossed their boundaries and started collecting data. Collection of these huge amount of data from the users have resulted in the generation of data mining. Marketers say that they keep the user's data private by viewing it only in aggregate, but the sheer volume of data a cookie can collect about any one person can enable the cookie's owner to infer a surprising amount of information about the individual being tracked.

Seizing cloud data – People tends to keep a backup of their videos, photos, important documents in google drive or other cloud based software. This is important especially because placing everything in the cloud allows you to access the information from anywhere and everywhere.

But on the contrary, storing everything on the cloud has bad implications also. The cloud services are provided by the third party hence privacy is a big concern. Companies collect these unauthorized data and use them for collecting information about the person. They do these for all the users. Companies are playing big these days by collecting the information and even small companies are paying the cloud service provides for getting accessing to these treasure trove of information.

Location data betrayal –Now-a-days people are addicted to the use of their mobile phones. Every mobile phones has a GPS system inside them which helps them to track down the location of a place. It also helps people to locate a place and

show directions to that place. It also shows the popular places nearby you.

People are overwhelmed with the usefulness of the GPS in their mobile phones but what they fail to see is that big companies are collecting location data from the users. They are using the location data to trace a person. When you keep the GPS system enabled on your phone while you travel, notifications pop up about the reviews of the places you visited. This is how the collection of the location data from the users is being implemented.

Data never forgets a face – People being proactive on social media often uploads pictures and tags other people in the photos for some innocent fun. But behind the scenes, it helps build a facial recognition database that makes escaping notice increasingly difficult for anyone. Considering the tech giants like Facebook, twitter, Instagram, where innumerable people post, tag and share other people's pictures and videos without even giving a thought that those pictures are being kept stored with themselves and can be used later to administer facial recognition algorithms on them to identify the person.

Scanning in the name of cybersecurity – This is an alternative name to network scanning. A computer, laptop or any digital gadget has a specific IP address. Whenever the network is connected to the digital gadget, a person sitting on the other side of the network can easily penetrate your firewall system and acquire information about the person sitting on the other side of the network. Unauthenticated scans reveal vulnerabilities found in the services running in the digital machine, open ports on devices that could allow malicious apps to run or communicate on them and configurations that affect the security.

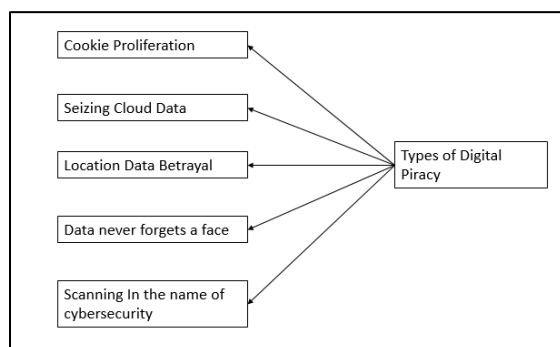


Fig. 2: Types of Digital Piracy

Steps to prevent digital piracy

Registering the work in a timely manner – Once you have made up your mind to continue with the work, a timely registering of the work is a necessary step to prevent your work to be copied or pirated by others. Getting a copyright for one's work is all about legally and rightfully protecting

one's work. If any person tries to pirate the copyrighted work, he/she is subjected to penalty under the law of that country.

There are many organizations globally, who have the right to register your work. One of them is Intellectual Property Rights cell (IPR). It has its headquarters in Mumbai with its other branches located at various parts of India like Kolkata, Bangalore, Mumbai. At a global level, organization named World Intellectual Property Organization (WIPO) is an agency of the United Nations to look after patenting and copyrighting of the new inventions and discoveries made.

Proactively monitor the internet–It is not enough to only copyright your work and provide protection to it. It is necessary to actively monitor the internet to see if anyone has pirated your work or not. Using an online monitoring service like MarkMonitor or Attributor can be useful to collect intelligence about the extent of the privacy problem. This can be performed by an individual or a group of people. Sometimes an individual hires and trains a group of people in that software and makes them proactively monitor the internet.

Tightening up of the licenses and the contracts – Proper copyrighting license and contracts are the only ways to keep the work safe and pirated free. So the owner or an individual should be very proactive in keeping up with the license expiry dates and renewing contracts. We cannot say that it is the responsibility of only the owner of the work. It is also the responsibility of the various organizations, providing licenses and contracts, to constantly be in terms with the owner and to constantly remind them that their licenses and contracts needs to be updated regularly.

A real life example of digital piracy-

With the global advent of the internet, distribution of the software over the internet has become the prime concern over the spread of pirated software. Prevention of the software distribution over the internet can greatly help in reducing the digital piracy.

Since the advent of the Napster in the year 1999, peer-to-peer applications has become very popular among a large crowd of people. A large group of people has started using the Peer-to-peer communications to download very large contents from the internet. An Internet traffic management firm has estimated that 50-65 percent of all Internet downloads traffic, and 75-90 percent of all Internet uploads traffic, are P2P-related. A peer-to-peer platform provides an excellent medium of sharing the digital media worldwide among common individuals. But it is illegal to use and especially to share the unauthorized digital media contents among others. One such example was BitTorrent.

BitTorrent is a peer-to-peer file distribution platform which is used to download and share large file and media contents

like movies, large videos, mp3 with minimal demand on the hardware resources and communication bandwidth. A BitTorrent network is made up of four types of entities – *Tracker* – It is the information center from where the peers can connect directly by obtaining the necessary information and download the files. It coordinates the distribution of files over a wide range of users.

Torrent file – It is a file that contains the metadata about the files to be shared among the peers. It also contains the address of the Tracker which is responsible for communicating to the peers.

Peer – It is a computer that is participating in communicating to the Tracker and downloading the large media file contents. All the peers sharing a torrent together is termed as a swarm.

Seeder – It is a peer that has already completed the downloading of the media files and now it acts as a Tracker allowing other peers to connect to it for downloading.

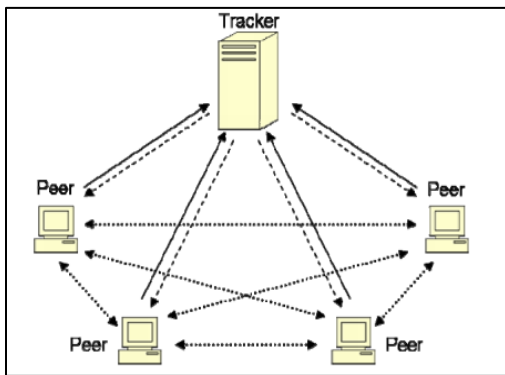


Fig. 3: The BT network working protocol in a swarm of 4

For sharing a file over the BitTorrent, the file owner needs to generate a torrent file which contains information such as the metadata about the file to be shared and the URL of the Tracker. After the creation of the torrent file, it is registered with the tracker and the file owner now has to make the torrent file available to other internet users by placing it on the website or anywhere else. The computer with the initial copy of the file is known as the initial seeder. After downloading the torrent file from the internet, a user opens it with a BitTorrent client program, which connects itself to the Tracker and is responsible for managing the transfer of the files. The BitTorrent protocol splits the file into a number of pieces of predetermined length. When a file is initially shared, peers do not have complete pieces to share with other peers. They need to connect themselves to the initial seeder and then request the pieces. As more peers start appearing, they begin sharing pieces with one another, instead of directly downloading it from the seeder.

A BTM system can be used to locate the Torrent file. It searches the target websites specified by user inputted URL. BTM is able to locate the Tracker and retrieve the lists of peers currently participating in the torrent. It continues to connect to the peers and gather data from each of them using the peer wire protocol. BTM consists of two modules – Torrent search and Torrent analysis, implemented in software components Torrent searcher and Torrent Analyser, respectively. Torrent Searcher is responsible for searching the torrent files on the website specified by the user and the downloaded torrent files will be passed down to the Torrent Analyser. Torrent Analyser is responsible for getting in touch with the trackers and the peers and gathers information on which analysis has to be performed.

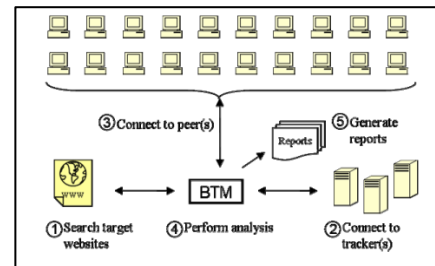


Fig 4: An overview of the BTM system

A Depth First search with a finite depth is adopted in BTM to maximize the number of torrent files located within a predefined stopping time. BTM performs automated torrent searching by seeking the torrent files on the website and exploring the hyperlinks over there. On each page indicated by the hyperlinks, it continues to seek the torrent files until a predefined level has been reached. A level with depth equals to three means that Torrent Searcher will catch hold of all the pages specified by the inputted URLs along with all those that can be accessed in two clicks on any link from there.

Torrent files will be downloaded and archived locally in the BTM system, on completion of the torrent file search. The processing is then passed to the torrent analyser which will then communicate with the trackers and peers using the BT protocol to gather information in the swarm. The Torrent Analyser then connects itself to the Tracker and then retrieves the information about the list of peers currently participating in the download. A rule system has been developed and incorporated into the BTM system. An alert will be prompted or sent to the pre-specified email addresses when a certain rule is satisfied.

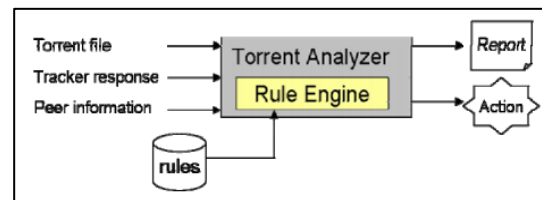


Fig 5: An overview of the Torrent Analyser

III. Future Works

Since 2007, there has been a rise in the digital piracy. Everywhere videos are being downloaded or online streamed in that case. It has become increasingly important to control digital piracy and impose strict rules and regulations for it. As it involves digital contents which are available on the internet, it becomes difficult to even reach the origin of the problem. Proper algorithms needs to be developed to reach the Tracker of the videos and the cyber security people should have appropriate control over the internet so that it can remove the digital contents from the internet as soon as any contents of digital piracy is posted. Also, people should not be allowed to download the pirated contents. Rules and regulations should be strict enough to prevent the selling of pirated contents. There have been cases where people are dwelling on the selling of the pirated digital contents. Organizations need to be developed whose sole purpose will be to maintain a database of the copyrighted digital contents so that the pirated contents can be differentiated. If we dig deep into the matter, we will be able to see that the people who are responsible for pirating the digital contents are technologically ahead of the organizations. So, by the time the cyber security people are reaching the digital contents, it has already reached out to a huge mass of crowd online as well as offline.

IV. CONCLUSION

The purpose of this study is to identify factors that influence an individual's attitude toward the decision to commit digital piracy. This study examines the factors that influence the attitude regarding such a behaviour. By doing so, measures to alter those factors can be implemented (and thus influence behaviour indirectly) that would reduce digital piracy – a current problem. This is especially important since many studies have suggested that individuals do not see piracy as a crime or an unethical issue. A better understanding of these factors that influence attitude toward digital piracy could prove to be essential in our understanding of this phenomenon and help us combat digital piracy. An examination of the cognitive beliefs held by subjects, as well as the other variables studied in this research could further help in combating digital piracy; for example, attitude toward piracy could be altered. Some beliefs held by subjects include – digital media is overpriced and lack of fear of getting caught.

Efforts to improve security will require strong technical leadership. Otherwise, standards efforts will tend to degenerate into unwieldy and ineffective committees with short-term focus. Leadership is also needed to prevent ineffective proposals from wasting time and momentum, to verify that security needs are met before products ship, and to help secure designs succeed in the marketplace. We conclude that only rights holders can provide this leadership; no other participants have the motivation, expertise, or

resources to ensure the deployment of effective anti-piracy technologies.

Most of the software activations are performed at user end, such as key validation and hardware integration, so anyone can easily get a hold on executable software and perform some tapping activity that can easily lead to overcome this activation or validation process. This problem can be related to finite state machine problem where every state of object can be examined and these states can be varied, ultimately to achieve a success state. Time and efforts after some attacks result in cracking. The disadvantage of static protection mechanism is that, once a copy is available that undoes the static copy protection or no longer carries the identification of the perpetrator, it can be distributed virtually to an unlimited extent due to which the software provider can no longer enforce its copyright. In short it is the static nature of existing defence mechanisms that are reason for them to fail.

REFERENCES

- [1] Sulaiman Al-Rafee, Timothy Paul Cronan, "Digital Piracy: Factors that Influence Attitude Toward Behaviour", 2006
- [2] Paul Kocher, Joshua Jaffe, Benjamin Jun, Carter Laren, Nate Lawson, "Self-Protecting Digital Content", 2003
- [3] B. Srinivas, Dr. Koduganti Venkata Rao, Dr. P. Suresh Varma, "Piracy Detection and Prevention using SIFT Based On Earth Mover's Distance", 2012
- [4] K.P. Chow, K.Y. Cheng, L.Y. Man, Pierre K.Y. Lai, Lucas C.K. Hui, C.F. Chong, K.H. Pun, W.W. Tsang, H.W. Chan, S.M. Yiu, "BTM – An Automated Rule-based BT Monitoring System for Piracy Detection", 2007
- [5] A. Parker, Peer-to-Peer in 2005, CacheLogic Research, available at http://www.cachelogic.com/home/pages/studies/2005_01.php
- [6] BitTorrent Protocol, BitTorrent.org, available at <http://www.bit-torrent.org/protocol.html>
- [7] Yawei Zhang, Lei Jin, Xiaojun Ye, "Software Piracy Prevention: Splitting on Client", IEEE International Conference on Security Technology, December 13-15, 2008
- [8] H. Chang and M. Atallah. Protecting software code by guards. Security and Privacy in Digital Rights Management, LNC S, 2320:160–175, 2002.
- [9] George Coulouris, Jean Dollimore & Tim Kindberg. Election Algorithm, Bully Algo & Ring based algo. In Distributed Systems, 2006
- [10] A. G., Galletta, D. F., & Thong, J. Y. L. "Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems*", 2003
- [11] Leugimap, Why "Free Software" is better than "Open Source", <http://www.gnu.org/philosophy/freesoftware-freedom.html> Free Software Foundation. October 6, 2004.