International Journal of Education and Research
Vol. 1 No. 1 January 2013

SOFTWARE PIRACY

D.Seetha Mahalaxmi,
Associate Professor,
Department of Computer Science,
JNTUHCEH, Kukatpally,
Hyderabad - '85

Dr. S. Viswanatha Raju,
Professor,
School of Information Technology
JNTUH, Kukatpally,
Hyderabad - '85

Dr. A. Vinay Babu,
Director,
Dept. Of Admissions,
JNTUH, Kukatpally,
Hyderabad - '85

ABSTRACT

We can see in the present grown up information technology a large number of attacks have been created by the attackers. In this paper a brief discussion of various attacks on software were given finally we are given an introduction to the attacks that are possible on software watermarking, such as additive attack, subtractive attack, distortive attack, and recognition attack.

KEYWORDS

Software watermarking, additive attack, subtractive attack, distortive attack and recognition attack

1. INTRODUCTION

In the present of Internet, software piracy has become a very common act. According to survey reports the software piracy resulted in lost revenue of nearly 30 billion dollars [BSAIDC]. It was estimated that piracy to be as high as 92 percent in some countries. Based upon these statistical results the researchers started to focus on software protection.

There are various software attacks, some of which are discussed in this paper. In this paper a detailed study on software attacks were given.

2. SOFTWARE ATTACKS

Software attacks [RKET] have been occurring in which malware or malicious software tried to infect computers. Cybercrimes are involved mainly with the malware attacks to make money and they make this possible via Internat. There are various software attacks. Some of which are discussed below.

2.1 Malicious Software or Malware

It consist of programming designed to disrupt or deny operations, which leads to information loss. It also allows gaining access to unauthorized access to system resources. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest, adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program.

2.2 Shadow software attack

The shadow software attack is based on the concept that an attacker could simulate the look-and-feel standard, launched by the victim, to steal user's personal information.

2.3 Various other attacks

Other types of attacks that are possible on the software are Virus, Worm, Trojan horse, Back Door (Trap Door), Logic Bomb and so on.

Virus is a Computer code that performs malicious actions by attaching to another computer program. Worm is a Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another program. Trojan Horse is a Software program which hides in another programs and reveal their behavior only when they are activated. Back Door (Trap Door) is a Password, known by the attacker, that allows the attacker to access a computer system at will, without having to go through any security procedures. Logic Bomb is a segment of the code that is embedded in organizations exiting computer programs, which gets activated and performs a destructive action at a certain time or date.

3. CRYPTOGRAPHIC ATTACKS

Cryptographic attacks are those which attacker performs on the cryptographic systems. Some of the cryptographic attacks are, Password Attack Dictionary Attack, Brute Force Attack, Denial-Of-Service Attack, Distributed Denial-Of-Service Attack, Phising Attack, Zero-Day Attack.

Password Attack Dictionary Attack is an attack that tries combinations of letters and numbers those are more likely to succeed, such as all words from a dictionary. Brute Force Attack is an attack that tries massive computing resource to try every possible combination of password options to uncover a password. Denial-Of-Service Attack, are the attacker sends as many requests as possible so that the target cannot handle them successfully and finally crashes. Distributed Denial-Of-Service Attack, is a first a set of computer are taken over by an attacker by using malicious software. These computers are called zombies or bots. The attacker uses these bots to deliver a coordinated stream of information requests to a target system, causing it to crash. Phising Attack is an attack that use deception to acquire sensitive information by masquerading as official looking emails or instant messages. Zero-Day Attack is an attack take advantage of a newly discovered, previously unknown vulnerability in a software product. The attackers take the advantage of vulnerability before the software vendor can prepare a patch for the vulnerability.

4. ALIEN SOFTWARE

The alien software of pestware, which is secret software that is installed in the computer through duplications methods and report web surfing habits and other personal behaviors. It does not have uninstaller program. The alien software are: Adware, Spyware, and Spamware.

Adware is software that is designed to help pop-up advertisements appear on the computer screen. Spyware is a software that collects personal information about users without their consent. There are two types of spyware namely keystroke loggers and screen scrappers. The keyloggers, records the keystrokes, and web browsing history. Eg: theft of password and sensitive personal information such as credit card numbers and recording the internet search history for targeted advertising. The screen scrapper records a continuous movie of screen contents. Spamware is a pestware that is designed to use the computer a lunch-pad for spammers. Spam will be sent to everyone in the email address book. Cookies are small amounts of information that web site stores on the computer, temporarily or more-or-less permanently.

5 CYBERTERRORISM AND CYBERWARFARE

Here attackers use a targets computer systems, via the Internet, to cause physical, real-world harm or disruption. Cyberterrorism typically involves individuals or groups, whereas cyberwarefare involves nations.

6. SOFTWARE WATERMARKING

Software Watermarking, protection is provided to the software by embedding a secret information into the text of software. The watermark helps to prove the ownership in the case of disputes. A brief survey of Software watermarking were discussed in the papers[ZYNN03][ZTW05].

Software Watermarking is a technique to embed a secret message into a cover message [CC][CC98]. Fingerprinting is a similar to watermarking, except a different secret message is embedded in every distributed cover message. This may allow us not only to detect when theft has occurred but also to trace the copyright violator.

6.1 Definition

Embed a structure W into a program P such that W can be reliably located and extracted from P even after P has been subjected to code transformations such as translation, optimization and obfuscation.

7. ATTACKS ON SOFTWARE WATERMARK

The various attacks that are possible on software watermark are additive attack, subtractive attack, distortive attack, and recognition attack.

7.1 Additive Attack

In additive attack adversaries embed a new watermark into the watermarked program, so the original copyright owners of the software cannot prove their ownership.

7.2 Subtractive Attack

In subtractive attack, adversaries remove the watermark from the watermarked program, without affecting the functionality of the watermarked software.

7.3 Distortive Attack

In distortive attack, the watermarked program is modified by the adversary so that the watermark cannot be extracted by the copyright owners and still keeps the usability of the software.

7.4 Recognition Attack

In recognition attack, adversaries modify or disable the watermark detector, or its inputs, so that it gives a misleading result. For example, an adversary may assert that his watermark detector is the one that should be used to prove ownership in the test.

8. CONCLUSION

In this paper we have discussed on various software attacks such as malicious software attack, shadow software attack, cryptographic attacks, Alien Software such as adware, spyware, spamware, Cyberterrorism and Cyberwarfare, Software Watermarking attacks such additive attack, subtractive attack, distortive attack, and recognition attack.

REFERENCES

1. [BSAIDC] BSA and IDC “BSA and IDC Global Software Piracy Study”, http://www.bsa.org/usa/research/, Nov,22,2004.
2. [CC 98] Christian Collberg, Clark Thomberson, “Software Watermarking: Models and Dynamic Embedding”, In ACM SIGPLAN - IGACT Symposium on Principles of Programming languages (POPL98), San Antonio, Texas
3. [CC] Christian Collberg, Clark Thomberson, On the Limits of software watermarking,
4. http://www.cs.arizona.edu/collberg/Research/Publications
5. [RKET] Rainer, Kelly R, Jr. and Efraim Turban, "Introduction to Information Systems", (2nd dition), p77-79. http://pmaungmaung.blogspot.com/2009/02/software-attacks.html
6. [ZTW05] W.Zhu, C.Thomborson, and F-Y.Wang, “A Survey of Softwrae Watermarking”, in IEEE ISI 2005, ser. LNCS, vol. 3495, May 2005, pp. 454 - 458.
7. [ZYN03] L.Zhang and Y.Yang, X.Niu,S.Niu, “A survey on software watermarking”, Journal of Software, vol. 14, no.2, pp.268-277, 2003.