Laptop Theft Analysis for Digital Investigations

J. Kejiya Ran[#1] , S. Prem Kumar[*2], U. Ram Mohan[#3], C. Uma Shankar[*4]
[#1]*Asst.Professor, Dept.of.CST, S.K. University, Anantapur.*
[#3]*Supdt. of. Police, Cyber Crime, Hyderabad.*
[*2]*HOD, Dept. of. CS, G.Pullaiah Engineering College, Kurnool*
[*4]*Professor, Dept. of OR& SQC, Rayalaseema University, Kurnool*

ABSTRACT: *The Study of computer security and certain aspects of cyber crime fascinated the detailed study of the present day most commonly encountered cyber crime like Laptop theft. In this paper, we present a novel methodology to encounter the Laptop thefts/ thievery. The principle adopted in this paper is basically a theft of a laptop/stolen/lost is to retrieve a stolen Laptop. The software is embedded into laptop and on the desktop pc and in case of the theft the information will be displayed on home desktop the moment laptop put to use. When stolen computer connects eventually to the Internet, it will report to a secret monitoring website and the suspect will be trace and caught. To reduce the loss of laptops in any organization , the laptops are connected to the main server where in a laptop is tagged with a card similar to an access control "Proximity card" .*

Keywords: *Computer Security, Cyber Crime, Embedded software, Proximity card.*

INTRODUCTION

Computer Security risks have become a topic of interest to people who use and rely on computers for various reasons. As computers become more vulnerable to damage , loss , theft and computer risk. In less than one generation, the information technology revolution has introduced the computer in to virtually every critical dimension of our daily lives and the economy. The new age carries within it a new peril. All computer driven systems are vulnerable to intrusion & destruction and even where all possible steps have been taken to make intrusion virtually impossible , a loss of service through connectivity can be almost as critical, albeit that safety is not a factor. A concerted attack on the computers of any one of our key economic sectors or governmental agencies could now have catastrophic affects. Therefore a comprehensive understanding about computers, their use , misuse has become an absolute essential for any law enforcement personnel. History is filled with competition between those who commit crime and those who try to prevent crime. This competition is a never-ending test of who can best create a new solution. There is no other form of crime that cuts so broadly across the types of criminals and the severity of their offences. Even though there has been substantial publicity in recent years about computer systems risks and attacks, it turns out that most system penetrations go unreported. Throughout history, each technological advance has become the target of those who seek to subvert it or use it for selfish purposes. Today, the spread of computer crime has touched nearly every form of occupation. It is estimated that within the next decade nearly all crimes will involve the computer in some way or other. Thus it has become inevitable for the law enforcement agencies to answer this most urgent need of the hour, tackling of Computer Crime.

COMPUTER CRIME

Computer crime can be defined as crime against an organization or an individual in which the perpetrator of the crime uses a computer or any computer enabled technology for all or part of the crime. Computer crime can be broadly divided into the following categories as per Interpol classification.

CATEGORIES:

Category I: Unauthorized Access Interception
A. Hacking B. Interception C. Time Theft

Category II: Alteration of Computer Data
A. Logic Bomb B. Trojan Horse
C. Virus D. Worms
E. False Data Entry (Data Diddling)
F. Salami Technique G. Trap Doors
H. Data Leakage

Category III: Computer Related Frauds
A. Cash Dispensers B. Computer Forgery
C. Program Manipulation D. Program Piracy
E. Fraud at Payment Points.

Category IV: Unauthorized Reproduction
Software Piracy

Category V: Computer Sabotage
A. Hardware Sabotage B. Software Sabotage

Category VI: Miscellaneous Computer Crimes
A. Theft of Trade Secrets
B. Distribution of antisocial Material
C. Eavesdropping and spying
D. Masquerading (Impersonation)
E. Piggybacking and tailgating
F. Scavenging and reuse

G. Scanning
H. Asynchronous attacks
I. Computer Component thefts.

PROBLEM OF INVESTIGATION:

The study of computer security and certain aspects of cyber crime of the present day like laptop theft is encountered with the advances in the technology and the adoption of computer technology to day today activity even by the common man, it is the dire necessity to provide minimum security measures to the common user. With the advent of technology becoming cheaper ,which very fact is being exploited by the common commuter ,where in the adoption to these computing technologies proving to be higher and higher with the literacy to understand the latest technological developments to their advantage and application in their daily lives for better quality of life, it is the need of the hour to protect the advanced electronic gadgets from any sort of shortcomings due to Software, Hardware problems, security problems like theft and others.

LAPTOP THEFT ANALYSIS:

Laptop theft is one such computer crime and an intellectual property loss which are rarely made public. It is learnt with great interest the statistics on laptop theft published each year by computer insurer Safe ware Inc. Even as the statistic topped a whopping above 6,20,000 laptop thefts, few people voiced concern. Recent data shows the value of the intellectual property assets lost with those thefts has grown rapidly, threatening to ignite shareholder cries of poor corporate asset management. This is also true for the loss of confidential data, particularly from financial industry firms. Asset mismanagement has far reaching implications these days.

Fortunately, one of the newest technologies for corporate security and supply chain now offers a solution, and that solution is now becoming mandatory. Radio frequency identification (RFID) technology has now been implemented successfully by enterprise and government IT executives to stem the alarming incidents of laptop thievery.

PRACTICES AGAINST LAPTOP THEFT:

Depending on what is kept on a particular laptop, lack of proper security precautions allows a thief to easily acquire such information as personal bookkeeping files, documents containing passwords, addresses, as well as employee and customer information stored on company laptops.

INSIDE PROTECTION:

Passwords are no longer adequate to protect laptops. There are many solutions that can improve the strength of a laptop's protection. Full disk encryption (FDE) is an increasingly popular and cost-effective approach. Full disk encryption can be taken on from a software-based approach, a hardware-based approach, or both - end-based approach. FDE provides protection before the operating system starts up with pre-boot authentication, however precautions still need to be taken against cold boot attacks.There are a number of tools available, both commercial and open source that enable a user to circumvent passwords for Windows, Mac OS X, and Linux.

Passwords provide a basic security measure for files stored on a laptop, though combined with disk encryption software they can reliably protect data against unauthorized access. Remote Laptop Security (RLS) is available to confidently secure data even when the laptop is not in the owner's possession. With Remote Laptop Security, the owner of a laptop can deny access rights to the stolen laptop from any computer with Internet access.

PHYSICAL PROTECTION

A number of computer security measures have emerged that aim at protecting data. The Kensington Security Slot along with a locking cable provides physical security against thefts of opportunity.

MODUS OPERANDI OF THE PROPOSED METHODOLOGY

Laptop loss was the third most prevalent type cyber security attack or misuse, behind viruses and insiders abusing network access and the loss are the intellectual property law, software, procurement time, setup time and any lease payment owed. Until recently a common misconception was that the impact of a stolen laptop was directly related to the replacement price of a laptop, which continues to drop as technology advances. Public awareness About these thefts has slowly grown over the years as several high profile occurrences have brought the issue forward.

The principle adopted in this study is that there is potential to retrieve a stolen laptop – simply embed software in to the laptop to recover it when it is stolen. The idea is that when the stolen computer eventually connects to the internet, it will report to a secret monitoring website and the suspect will be trace and caught. To reduce the loss of laptops, in any organization the laptops are connected to the main server where in a laptop is tagged with a card similar to an access control “Proximity Card”.

Whenever a Laptop is stolen and when the burglar starts working with the laptop the information will be automatically be tagged on to the main server which gives the indication and where abouts of the burglar who can be traced while recovering the lost laptop. The system established in this work is being presented in the following Flow chart giving different permutations and combinations of connecting the burglar to the server. If more number of laptops are stolen the server can simultaneously track and trace the where abouts of the lost laptop and even hooking with the burglar.

DESCRIPTION:

The main server is connected to fixed number of clients (burglars). Now the first client (burglar) information is tracked by the server when the burglar starts operating the lost laptop. In the meantime a second bugler is found but can't be tagged on to the server as the first burglar has to say "bye". The burglars can't be tagged on to the server unless and until the concern say bye. To overcome this (if a burglar do not say bye), a timer will come into action and after fixed time the burglar on site of the server will automatically pave way for the next client (burglar).This procedure continues to as many burglars to the capacity of the server which is fixed i.e. "N". Code is been developed using java programming.

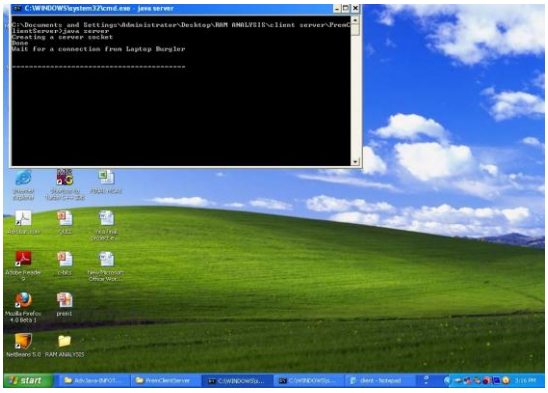
ANALYSIS:

Based on the description of the flowchart the proposed laptop theft analysis is a handy cyber crime tool to distinguish the laptop which is stolen / lost / misplaced etc.. The Analysis provide an advantage that the server (based on its capacity) can track finite number of clients (burglars) simultaneously. Tracking simultaneous clients is known as concept of Threading. Threading basically helps to meet the multitask demand. The number of clients to be tracked may be basically directly proportional to the capacity of the server and tracking 'n' number of clients is called as Thread Pool.While tracking the information of the burglar who may be tracked only once by the server or may be tracked for the second or third and so on for only' n 'fixed times.

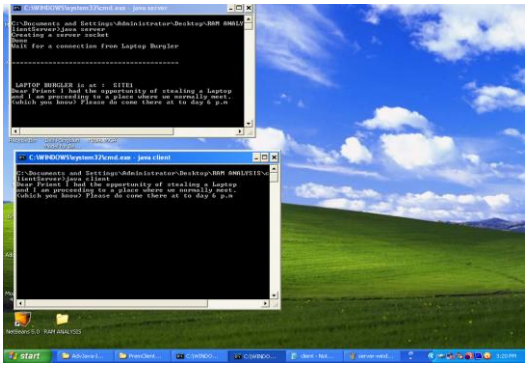
QUEUE NETWORK TRACKING PROBLEM:

The entire analysis can be viewed as a QUEUE NETWORK TRACKING PROBLEM as it can be designated as a single service channel Queuing system. This can be related to as an M/M/1 : F,FIFO System as the arrivals will be the calling clients(burglars) and with single server service facility where in the system can accommodate only finite number of clients and the calling clients service will be done on First come First service priority. This system can further be extended to a multiple channel case model as M/M/C to provide service through multiple servers if the calling customers is more than the capacity for a single server and here we have multiple waiting lines before each service channel. This kind of systems will once again can be extended to Priority based queuing systems as the service of the calling customers can be undertaken based on the priority of the client. This facilitates the cyber crime investigator to probe regarding the theft in a very convenient way and as a future course of work. The developed and reported Laptop Theft Analysis in this section can be modelled as Queuing Network Tracking Problems and providing solutions to such problems will increase the precision of the investigating analysis thus providing the required solution in the sense in nabbing the culprit.

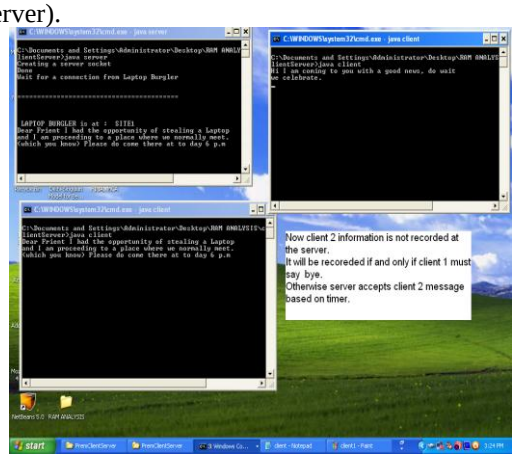
SCREEN SHOTS PICTURE1:



The first screen shot is the server
Beneath the server screen shot is the Site1 of the



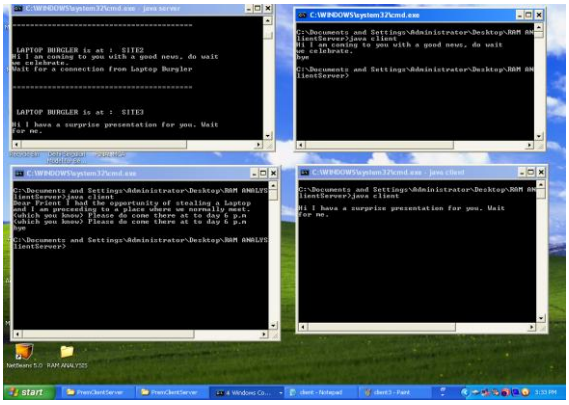
burglar1 with the information (which is tagged on to server).



The adjacent to the server screenshot is the information of the client2 i.e. Burglar 2.

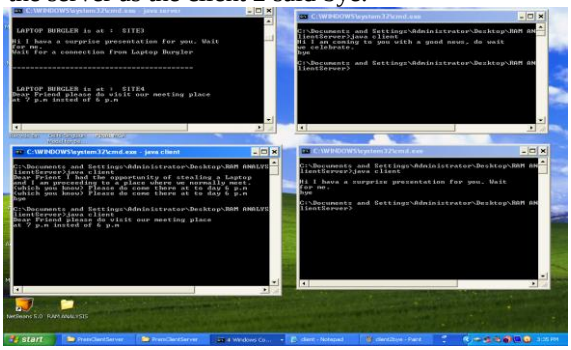
Now the client 2 information is not recorded at the server and it will be recorded if and only if client 1(burglar 1) must say bye. Otherwise server accepts client 2 (Burglar 2) message.

PICTURE 2:



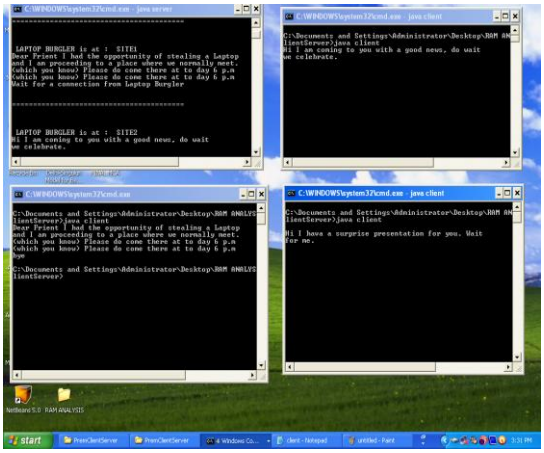
The first screen shot is the server. (site 2 with burglar 2 bye information).

The last screen shot of the picture is the information of client3 (burglar 3) which is tracked by the server as the client 2 said bye.



Beneath the server screen shot once again the client1 (Burglar 1) re entered with information and can't be tracked by the server for the reason that client 3 has to say bye.

PICTURE 3:



The first screen shot is the server at site 3 with client 3 information. Client 3 said bye.

Here at this stage client 1 is being tracked by the server with additional information at site 4 (but this information is related to client 1 at site 1). This is allowed to track information regarding the burglar and such re entry can be made by the burglar .

CONCLUSION:

This novel procedure developed in this work is highly useful in tracking the culprit who is responsible in stealing the laptop and as many as finite number of culprits can be tracked with the useful information which helps the cyber crime investigator to negotiate the where abouts of the culprit.

REFERENCES:

[1] BOCIJ . P et.al (2002) 'Cyber stalking : A new challenge for criminal law', 3-5,vol. 122, Criminal Lawyer.

[2] BRAIN D. CARRIER , JOE GRAND (2004) " A hard ware based memory acquisition procedure for Digital Investigations " 1742 – 2876 , Digital Investigation journal.

[3] CHAVALAS .B , PHILIPS . A (2005) Trojan Defence : A Forensic View Part II, Digital Investigation Journal.

[4] CHITTESTER C.G , HAIMES Y.Y(2004) Risks of Terrorism to Information Technology & to critical interdependent infrastructures. Journal of Homeland Security & emergency management.

[5] CHRISTOPHER BURGESS, RICHARD POWER (2008), " Notes on Cyber Forensics ", 297-304 , Secrets Stolen.

[6] COHEN .F (1999) simulating cyber attacks, defences & consequences. 479-518, Computers & Security.

[7] COLLIN B.C (1997) " The future of Cyber Terrorism : where physical & virtual words converge " , 15 – 18, crime & justice international.

[8] D.YEUNG, Y.DING (2003), Host Based Intrusion Detection using Dynamic & static behavioural models , 229-243,pattern recognition.

[9] DA-YU KAO ET.AL (2010) " Strategy of Triple –E on solving Trojan defense in cyber crime cases ", vol.26, 52-60, Computer law & security Review.

[10] DEVOST M.G et.al (1997) " Information terrorism : Political violence in the information age " , vol. 9 , 72 – 83 , terrorism & Political Violence.