Advanced Computing: An International Journal (ACIJ), Vol.3, No.4, July 2012

A New Approach to Theftware-Efficient Solution

Prabhat Kumar[1], Abhishek[2], Milan Jain[3], Niraj Upadhyay[4], Avinash Thakur[5]

[1]Department of Information Technology, NIT Patna, Patna, Bihar
prabhat8@gmail.com

[2] Department of Information Technology, NIT Patna, Patna, Bihar
aabhishek.nitp@gmail.com

[3] Department of Information Technology, NIT Patna, Patna, Bihar
milanjain81@gmail.com

[4] Department of Information Technology, NIT Patna, Patna, Bihar
niraj.nitp08@gmail.com

[5] Department of Information Technology, NIT Patna, Patna, Bihar
avinash.nitp@gmail.com

Abstract

Theftware is software cum a proposed firmware which helps to track down a laptop in case of theft. Now a days, cases of laptop theft are becoming too frequent and prominent as it's a pretty easy as well as rewarding affair for the burglars. Especially in the second and third world countries, where the hitherto technologies are not up to the international standards i.e. there is a big lacunae between the western countries and the developing countries in terms of technological infrastructure. In such places to prevent, stop, and track down of such cases of nuisance, we propose a model named Theftware which is a sine-qua-non as it's being developed with an eye that it's for the masses and not for the few selected. We also purpose a central server with a database of all the registered laptop users in the world which will be under the control of a government regulatory authority or it may be an autonomous one, depending on the requirements, need and power required to be vested in them. All the companies i.e. laptop manufacturers or service providers needs to enter all the details of their customers along with the information of laptop sold to them. The registered users in case of theft will report to this regulatory authority that will verify the request and report to the server if required. The work of Theftware starts from here as it periodically checks the central database to verify that the laptop has been stolen or not. If the laptop is found under scrutiny it will report to the server with the detailed information of its present location, so that it can be tracked by the regulating authority. In this paper we have proposed how an ordinary laptop can be vested with a Theftware process and how this process collects the system details along with the process of communication with the remote server. In this paper we have also discussed the scheduling algorithm for the Theftware which is a sine-qua-non for the laptop's efficient performance along with the algorithm for the various processes inside Theftware. We have also prepared a comparative study which shows the laptops performance degradation on vesting with this software.

Keywords

Pre-boot authentication, Centralized server, Remote login, Remote lock, Sysinfo.

DOI : 10.5121/acij.2012.3411

1. Introduction

According to the FBI, losses due to the laptop theft have been found more than $3.5 million dollars in 2005. The Computer Security Institute/FBI Computer Crime & Security Survey found the average theft of a laptop to cost a company $31,975.[13] The incidence of laptop theft has been growing along with the phenomenal use of the laptop. Around 2 laptops in every 10 laptops are stolen every day,[1] even having various sorts of expertise in tracking down these stolen devices at additional cost.

In a country like India which is arguably considered one of the largest market for electronic devices like laptops and mobiles. Their thefts are very serious and important issue to handle as an average citizen can't afford multiple laptops in case of one being stolen unlike their western counterpart nor they can spend that much money on buying expensive tracking mechanisms like Alerta Laptop[9] and Absolute software[7] which is not only expensive but presently not available in developing countries. Moreover the importance of data is increasing day by day and has already become more important than the laptop itself. Hence a mechanism of tracking stolen laptop so as to increase security has become a necessity. Further, this problem needs social views also and some sort of different mechanism is a must requirement which may deter future laptop theft. Theftware is an effort in this direction which fulfills both the concept of tracking as well as delimiting the laptop theft. Thefware is an effective as well as a viable option for the ordinary naïve users. Theftware can work as a deterrent for future reference and prove itself as an appropriate mechanism for theft cases.

2. Proposed Model

We propose a central server with a database of all the registered stolen laptop users in the world which will be under the control of a government regulatory authority or it may be an autonomous one, depending on the requirements, need and power required to be vested in them. All the victims of laptop theft will have to lodge a FIR to the local police station; the mechanism will be such that the FIR report along with all details of the laptop will be send by the police to the regulatory body, which will activate Theftware present in the stolen laptop registered in the central database.

The work of Theftware starts from here as it periodically checks the central database to verify that the laptop is under surveillance or not, If found under scrutiny it will report to the server with the detailed information of its whereabouts, so that it can be tracked by the destined authority.

3. Related Work

Intel's Antitheft Technology

Intel AT includes several hardware-based detection mechanisms that can trigger a lock down. Detection mechanisms can be local (based on IT policy) or remote (via LAN[22], WLAN, or 3G[3]connectivity).Two Hardware-based detection and trigger mechanisms (all configurable by flexible IT policies) include:

a. Excessive login attempts in the pre-boot authentication (PBA) screen.

b. Missed check-ins with the central server.

c. Notification via a message sent over an IP-based wired or wireless LAN.

d. Notification via an encrypted SMS text message over a 3G [4][5] network.

In the above case except case (d) the system goes in theft mode and starts an automatic hardware lockdown even if the system is booted or boot order is changed, and in the case of option (d) whenever it is in the 3G network range[10][19][20] it send a message to its server consisting of its GPS coordinates.

ASUS Anti-Theft

ASUS Anti-Theft[24] protection keeps confidential data safe and secure. It contains 3 level of protection to keep the highest safety for our laptops.

1) LOCATES AND TRACKS the stolen laptops- It's even possible to track and recover a laptop after it's been stolen, with the help of Comp trace LoJack software inside.

2) REMOTELY LOCK YOUR STOLEN LAPTOPS-Still, should all else fail, ASUS Anti-theft solution integrated with the Intel Anti-theft technology in chipset, so user can remotely lock the system and/or delete the data on the stolen computer, so there is never any risk of sensitive data ever being seen by the unauthorized people.

3) ANTI-THEFT SOLUTION always working even when the software is removed from the hardest - What guarantees the system works, is the fact that the Persistent Embedded BIOS Agent will always function, even if the hard disk is wiped or replaced, so there's no way to circumvent the protection. ASUS' Anti-Theft solution is built to always keep your data protected.

4. Drawbacks Of Related Work

The Intel Antitheft Technology works on concept of hardware lockdown by use of internal embedded hardware but in this case the laptop is merely can't be used but its tracking is not possible. In case of Intel Antitheft tracking is possible only when it is in the 3G network[6][8][18] range, which is not possible in case of developing countries like India as 3G network is not widely used, moreover the thief also knowing this will never expose his laptop to 3G network, moreover it works only on Intel's hard disk not on other manufacturer's hard disc and lastly the customer has to buy this mechanism and has to incur its yearly cost even if his/her laptop doesn't get stolen which is a overhead for middle class people.

Second major drawback of Intel Antitheft[2] is that it is available only for windows, so not compatible for every operating system like UNIX[21], LINUX and Fedora[17].

Asus Anti –Theft, for locating and tracking down of laptops require third party software. Comp trace LoJack is the software used which leads to serious concerns of degrading the efficiency of the anti theft system. It also uses Intel Antitheft technology so all the major drawbacks of Intel Antitheft are also carried over here.

In this there is persistent embedded bios agent is used. As a result, there is a requirement of larger ROM.

5. Working of Theftware

5.1. Process Boot-up

We have used a tracert command which periodically checks for the internet connection and on successfully sensing the network it calls up the Theftware program to collect system details and forward it to regulating authority.

5.2. Checking the status of the laptop

The process on finding the internet connection connects to the remote central server and generates a report containing all the system information in a text file saved on a secure location. This secured file has to be sent to our central server for tracking purpose as it is the main source of information regarding laptop location. In this step, we would also check the connection strength of the internet using a variable connLoss which contains a value indicating connection strength. This variable will be the main part for the entire process as everything depends on the value of this variable that whether system will send the file or not so that its delivery failure may be avoided.

5.3. Connection establishment and file sending

Now the sysinfo file has been generated, so now we need a connection of our laptop to remote server. Connection could be via two protocols either HTTP of FTP but using HTTP would not be a good decision as it needs better connection and difficult to establish, so we are using FTP that can also work in slow connections and is capable of working quite fast.

6. Implementation

The above concept is implemented showing algorithms:

Algorithm 1: Main() function

1: *connLoss* = 100;
2: change cmd prompt to System32;
3: **do**
4: tracert www.google.com and copy to text file *conninfo.txt*;
5: *connLoss*=Loss.datum;
6: **while(**connLoss≥50**)**
7: ipconfig/all and move data to *sysinfo.txt;*
8: create FTP connection and send *sysinfo.txt* to web space;

Above is algorithm for Main() module

Algorithm 1: This is the main() function algorithm where Theftware will check whether any connection is available or not and if it is available then next step would be checking whether that much of internet speed is sufficient for the transfer of sysinfo text file to our remote server for further processing. conninfo text file is about the information generated due to tracerting. We are tracerting a specific website i.e. www.google.com to generate connection report for the next step. This module of Theftware is utilizing maximum resources of our computer hardware. sysinfo text file contains all the necessary details about the system necessary for tracking purpose.

Assumptions: In this module we have assumed that a mean value for the loss equal to 50% as theftware is using dos command that will send four packets on the basis of which strength of connection would be determined. So we have chosen a mid-value that would be appropriate to send sysinfo file. In the beginning of module we have used a variable connloss that represents the connection lost and for the first time we have assumed that there is a proper network connection.

Algorithm 2: FTPMain() function
1: open;
2: *Name of Webspace*;
3: *username;*
4: *password;*
5: send file to webspace;
6: bye;

Above is an algorithm for FTPMain() module

Algorithm 2: Next module of Theftware works for creating a FTP[11][12][16] connection to send the file containing all necessary details i.e. sysinfo file. This will provide valid username and password authenticating the user.

Algorithm 3: Loss() function
1: *ch, i, datum*=0;
2: open *conninfo.txt*;
3: **while(***ch*≠'('**)**
4: get next character;
5: **end while**
6: move to next character;
7: **for** each i in current position to '%'
8: *datum* = convert to ASCII value;
get next character;
9: **end for**
10: return datum

Above is an algorithm for loss module

Algorithm 3: This is a function generating the loss in your internet connection. It is a necessity of Theftware to check whether present internet connection is of that standard or not. Slow connection may generate failure of text file which we want to avoid. Generated loss is stored in a variable which is passed to Main module of Theftware.

Assumption: In this module we have assumed that a conninfo file has been generated by the main module, so as to get value representing the strength of internet connection.

7. Performance Analysis

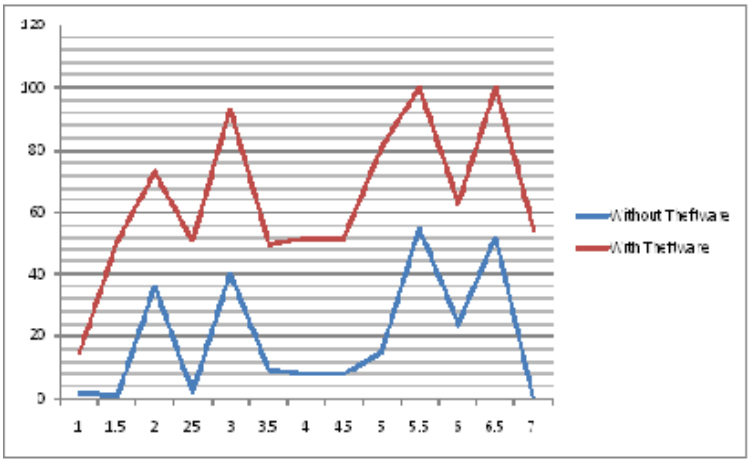

Figure 1. CPU Utilization

Above is a graph showing the comparison of CPU utilization with time when
a) It is vested with Theftware
b) It is not vested with the Theftware
in both the situation there is no internet connectivity

The blue curve is showing the CPU utilization when there is no Theftware running and the red curve is showing the same but with the difference that Theftware is running in the background

The comparative study shows that the CPU utilization increases with time which is shown by a variations in slope

$$X=m(Y-d)$$

Where X represents x-coordinate

Y represents y-coordinate
m represents slope of the line
d represents x-axis intercept

Then the CPU utilization is shown degrading with time with the equation

$$Y=m*X+c$$

Where X represents x-coordinate
Y represents y-coordinate
m represents slope of the line
c represents slope on Y-axis

8. Drawbacks

Theftware though quite efficient of handling laptop thefts, also has some drawbacks on which work is going on. First of all tracerting continuously capitalizes lot of CPU resources thus resulting in slow working of the computer. Also Theftware is capable of working on 32 bit systems till now. Theftware is compatible with Windows and lacks support for other OS like UNIX.

8. Future Work

This software has been developed on Windows 7, 32 bit operating system. The software would be enhanced to work on both 32 bit operating system as well as 64 bit operating system. Further improvements may empower the software to work on other operating systems like UNIX[14][15] ,LINUX etc. Future work may enhance the efficiency of the software. The software may also be optimized for Multicore processor. We are also having a scope of encrypting the text file sysinfo to increase the security in Theftware.

References

[1] Security Survey ^ *2005 FBI Computer Crime & Security Survey*

[2] http://www.intel.org/content/dam/doc/white-paper/anti-theft-technology-laptop-security.pdf

[3] Castiglione, A.; Cattaneo, G.; Maio, G.D.; Petagna, F.;, "SECR3T: Secure End-to-End Communication over 3G Telecommunication Networks" Publication Year: 2011 , Page(s): 520 – 526 IEEE Conferences, Seoul.

[4] Lei Zhao, Technology Trend: Construction of transmission network in 3G era. pp.241-242, December 2010.

[5] Frank Hartung, Uwe Horn, Jörg Huschke, Markus Kampmann, Thorsten Lohmar, and Magnus Lundevall "Delivery of Broadcast Services in 3G Networks" IEEE TRANSACTIONS ON BROADCASTING, VOL. 53, NO. 1, MARCH 2007. Herzogenrath

[6] Gu Shenghua.The strategy construction planning for 3G transmission network, Mobile Communications, VOL 31: pp.72-75 , 2007.

[7] http://www.absolute.com/en/lojackforlaptops/home.aspx

[8] 3G TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[9] http://www.alertalaptop.com/new/lang/en/index.php

[10] Houssos, N.; Gazis, E.; Panagiotakis, S.; Gessler, S.; Schuelke, A.; Quesnel, S.;" Value added service management in 3G networks" Publication Year: 2002 , Page(s): 529 - 544
Cited by: 1
IEEE Conferences, Issued at: Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP

[11] Wanbo Zheng; Shufen Liu; Zongwei Liu; Qingxing Fu;" Security transmission of FTP data based on IPSec" Publication Year: 2009 , Page(s): 205 - 208
IEEE Conferences, This paper appears in: Web Society, 2009. SWS '09. 1st IEEE Symposium on Issue Date : 23-24 Aug. 2009

[12] Liu Xia; Feng Chao-sheng; Yuan Ding; Wang Can;" Design of secure FTP system" Publication Year: 2010 , Page(s): 270 - 273
IEEE Conferences, This paper appears in: Communications, Circuits and Systems (ICCCAS), 2010 International Conference on Issue Date : 28-30 July 2010.

[13] http://en.wikipedia.org/wiki/Laptop_theft#cite_note-0

[14] Black, J.P.; Marshall, L.F.; Randell, B.; "The architecture of UNIX united" Publication Year: 1987, Page(s): 709 – 718, Volume: 75, Issue: 5

[15] Cardarella, D.E.; "UNIX concepts and capabilities" Publication Year: 1990, Page(s): 1 – 3,

[16] Griffin, D.; O'Reilly, F.; "Integrating SIP, presence and FTP to provide wireless multimedia messaging" Publication Year: 2004 , Page(s): 2581 - 2586 Vol.4

[17] Anbalagan, P.; Vouk, M.; "On Reliability Analysis of Open Source Software – FEDORA" Publication Year: 2008 , Page(s): 325 – 326,

[18] La Porta, T.F., Security and IP-based 3G wireless networks, This paper appears in: Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on Issue Date : 17-19 Oct. 2005,On page(s): 211,ISSN : 1095-2055

[19] Putz, S.; Schmitz, R.; Secure interoperation between 2G and 3G mobile radio networks, This paper appears in: 3G Mobile Communication Technologies, 2000. First International Conference on (Conf. Publ. No. 471) Issue Date : 2000,On page(s): 28 – 32

[20] Xie Yinfen; Planning of 3G-oriented transmission network. This paper appears in: Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference onIssue Date: 16-18 April 2011,On page(s): 5122 – 5125,Location: XianNing.

[21] Bishop, M.; Reflections on UNIX Vulnerabilities, This paper appears in: Computer Security Applications Conference, 2009. ACSAC '09. Annual Issue Date : 7-11 Dec. 200,On page(s): 161 – 184.

[22] Sicher, A. HiperLAN/2 and the evolution of wireless LANs, This paper appears in: Emerging Technologies Symposium: Broadband, Wireless Internet Access, 2000 , IEEE,Issue Date : 2000,On page(s): 1 pp.

[23] Tarkoma, S.; TSR: Temporal Subspace Routing for Peer-to-Peer Data Sharing, This paper appears in: Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE Issue Date : Nov. 27 2006-Dec. 1 2006 On page(s): 1 – 6

[24] http://www.asus.com/Notebooks/Features/ASUS_AntiTheft_Solution

Authors

Prabhat Kumar Assistant Professor, Department of Information Technology, NIT Patna, Patna, Bihar

Abhishek Department of Information Technology, NIT Patna

Niraj Kumar Upadhyay Department of Information Technology, NIT Patna

Milan Jain Department of Information Technology, NIT Patna

Avinash Thakur Department of Information Technology, NIT Patna