*Oriental Journal of Computer Science & Technology* Vol. **1**(1), 81-88 (2008)

# Failures of network security utilities

**MANDAVA V. BASAVESWARA RAO and CH. NAGA MANISHA**

GITAM University, Visakhapatnam -530 045 (India)

(Received: February 12, 2008; Accepted: April 04, 2008)

**ABSTRACT**

Main aim of network securities is to maintain confidentiality for the user sensitive data. For this purpose, there are lot many Network Security utilities are available in the market for securing the user data. But no utility is proved perfect for securing the system. Because threats are either by wrongly motivated human activities or highly powerful threats introduced at any moment. Every moment threats greatly challenges the systems.

**Key words:** Net work securities**,** Anti Threats, Less System Knowledge, Updating Problems, Human actions.

## INTRODUCTION

Networking is to secure the confidential data of the user from the other users. Lot many threats challenging the network security system at every moment. For this reason, to increase the security for the system user installs different security systems. These security utility failures are reported most frequently due to wrongly motivated human activities or powerful threat enter into the system, which are more powerful than the security utility.

**Why secure our system?**

The main aim of the every security program is to maintain confidentiality of user data and also to secure data. To hide the user data from other users, and protect and expose the data to the targeted users only. Based on these goals many system secure programs are developed by different companies. But none of the programs protects users perfectly, due to the fact that the day to day more powerful threats are developed by the selfish motivated people.

**Network security system problems**

Systems generally face problems when connected to network. Lot of threats fight with network security systems to enter into user's systems. Some threats may corrupt the system or files. Some threats may take the all control over the system. Some threats may steal the users sensitive data which is known as Hacking".

**Why hacking the user's data?**

To know the users personal data that is, user information, passwords for hacking the email ids and other details. Hacking the credit and debit card numbers for online shopping. And also for hacking the user videos and photographs for morphing.

**Hacking techniques & threat to the securities systems**

Various techniques are used to hack the data.

**Trojan horse**

A Trojan horse is a malicious code. It is a harmful programme. Trojan infections are different from system to system. When a Trojan is activated on the system it may change the settings of the system that may change the desktop information, or add active desktop icons. The

Trojan horse may delete or destroy the system files and information on the system. Present days the Trojan horse are widely increased and challenging the network security systems in big way.

Trojans are very familiar as a backdoor to enter the user system that gives other users that is, hackers easily accesses the confidential and personal information of the user.

The Trojan Horse comes from the a Greek story of the Trojan War, in which the Greeks give a giant wooden horse to their foes, the Trojans, as peace offering. Once Trojans drag the wooden horse inside their city walls, Greek soldiers come out of the horse's hollow belly and open the city gates, allowing their soldiers to pour in and then subsequently capture the city.

**Types of trojan horse**

**Remote access trojans**

These Trojan horses hide in games or in other small applications. When the user execute these programs these Trojan horse enters into the system. This Trojan also gives complete control over the system to the hacker.

**Data sending trojans**

This type of Trojan horse aim is to attack the sensitive data of the user. It attacks the user password, credit card information, log - files, e-mail ids or messenger contact lists etc. These Trojan horses may installs keylogger in the user's system. Keylogger means read every keystroke of the user and record the data into the file. The keylogger sends the recorded keystroke files to the attacker.

**Destructive trojans**

This type of Trojan horse aims to attack on the main important files. This Trojan is delets or destroys the files. It is more like a virus. It is even not possible to detect by the Anti-Virus Software.

**Proxy trojans**

This type of Trojan horse aimed to use the user system as a proxy server. Using this Trojan the, attacker can access all the data from the user system. That is, the attacker can fraud the credit card numbers etc., and other illegal activities or even they do hacking the data from other systems or launch the harmful code into the other networks or the systems. This is useful for illegal activities. Makes the owner of the system responsible for all these illegal activities.

**FTP trojans**

This type of Trojan horse aims to attack to open the port and connect to the user system using the File Transfer Protocol (FTP). The Trojan opens the port 21 for connecting the user system, since the port 21 is used for FTP transfer.

**Security software disabler Trojans**

This type of Trojan horse aimed to attack on the security programs such as anti-virus, anti-spyware or firewalls etc. This Trojan is used to stop or kill security programs without the user knowledge.

**Denial-of-Service attack (DoS) Trojans**

This type of Trojan horse aimed to attack on network. It is designed to bring the network to its knees by flooding it with useless traffic. The Denial-of-Service attacks such as the ping of death and teardrop attacks.

**Virus**

Virus attacks program or file and it can spread from one system to another system. virus infects every system when they enter into the system. The viruses damage user hardware or software or confidential information of the user in the system or the system files of the system. All most all viruses are attached to executable files that are .exe files. When the user executes file then only the virus will infect the system. The virus is spreads into the systems via email attachments, CDs, DVDs, pen drives and floppies etc. Or when the user shares the data, that also spreads virus.

**Worms**

A worm design is similar to that of virus. It is considered to be a piece of a virus. But the main difference is virus spread from one system to another system with human actions, but a worm has a capable to spread from one system to another without any help from human actions. A worm takes advantage of file or information transport features on system, which allows it to travel unaided. The biggest danger with a worm is it is capable to

replicate itself on user system, so rather than system sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. The coping nature of the worm makes it capable to travel across networks. This may cause loss of system memory. It has capability to stop the response of the web servers, network servers and individual systems.

**For example**

A worm to send a copy of that worm to every one listed in address book in emails. Also in mobiles it sends worm messages to everyone in the phonebook.

**Phishing attacks**

Phishing is an attempt to acquire sensitive information, such as usernames, passwords and credit card details, when the user enter these details in electronic communication. Online shopping and online bankings are common targets. Phishing is typically carried out by e-mail or instant messaging and often misdirects users to enter the details on website.although phone contact also been used.

**For example**

If a person wants to know friends password, then they send a fake login page. Then the user (friend) thinks that his/her mailbox is logout. So, the user once again login the page in fake login page sent by the hacker, with the username and password. So hacker uses this way and gets the user name and pass word which can be used at any time with out the knowledge of the original user.

**System security utilities**

**Utilities**

A program that performs a very specific task, usually related to managing system resources. Utilities differ from applications mostly in terms of size, complexity and function. For example, word processors, spreadsheet programs, and database applications are considered applications because they are large programs that perform a variety of functions not directly related to managing system resources.

**Security Utilities**

Security Utilities main aim is to secure user data from other users. The Secure utilities are used to fight with malicious programs and protecting the system.

**Types of security utilities**

**Anti-Virus**

Anti-Virus is a utility to search the system for the files which are infected by the virus.

**Anti-Spyware**

Anti-Spyware software is a program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.

**Anti-Spam**

Refers to software, hardware or process that is used to combat the proliferation of Spam or to keep Spam away the system.

**Firewalls**

Firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. A firewall's basic task is to regulate the flow of traffic between computer networks of different trust levels.

**Why network security system utilities fails?**

There is no exact proof for the failure of the network security programs. The network security system fails not only because of the faults in the program but also due to miscellaneous using of the system. There are many occations network security system utilities are failed. This is the main reason makes every system user searching for the best security system utility.

**Reasons**

**Users lacking system knowledge**

Due to the improved awareness and convenience almost every body started using the system for various purposes. There are nearly 40% of the users having knowledge about system remaining 60% users are not having sufficient knowledge about the system. So most of the users are confused with the security systems. Users

installed different firewalls and anti-virus etc for the security purposes. But when some programs used to process the secure systems warns even though there is no threat. Then most of the users confused about the warning due to the lack of system knowledge and they are confused whether to enter the allow or deny options.

Figure. 1 shows the example for this situation. Comodo firewall is good and highly rated

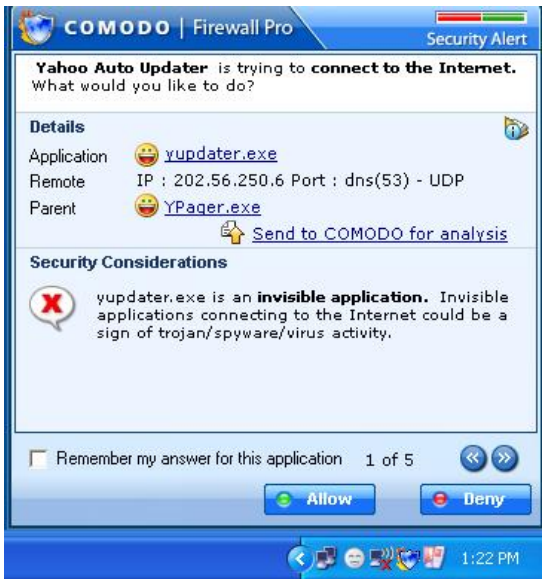


**Fig. 1**

software for the secure the system. When the user login to the famous messenger Yahoo… yahoo trying to update their software, the firewall warns that "yupdater.exe is an invisible application, this may sign to Trojan/spyware/virus activity". But user may confuse whether to allow this process or deny it!!?. In this situation they think if they allow it, it may contain any threats that infect the system. If the user denies the process, user may not be able to exploit new features of the yahoo messenger.

If the firewall is given option to block all the programs that contain the threats without any notice, Then the user may loss the important data, and it may not be possible to recollect the data. Since the utility immediately block the yupdater.exe and the user loose the new features of the yahoo messenger.

**User not update the security systems**

Many people are not giving the importance to updating the security systems. They are not aware of the expired of the secure programs. This cause the threats are easily enter into the system. For example most of all the anti-virus soft wares maintain the database for the virus information. When they detect any files similar to the information of the file in the database the program can easily remove or destroy or correct


**Fig. 2**

the file and protect the system from harmful codes. But when the user not to updating the program, the program does not know about the present threats. If the secure utility may found the threat then the secure program has unable to correct or delete the file. Since the secure program has no capacity to remove the threat from the system. Fig. 2 shows this example.

**Secure program may be a threat**

There is lot of secure freeware and shareware programs available in the online. All most all users are give preference to install the freeware software. This is a very big advantage for the threats. When the user installs any firewall or any anti-virus software, the software warns the user to stop third party firewall or anti-virus software.

If the user stop the previous secure programs and install the new one. Then only the

new software is protecting the system. This reason if the new program may hack the data or infect the system the user cannot identify the data may hack because no other programs detect the hacking, Because they are in off mode.

If the user cannot stop the previous secure programs the two secure programs fight to each other and they are trying to block each other programs. This causes the system has no correct protection.But some situations some secure software warns another secure programs are malicious programs.This situation user confused about the software. For example Spyware Terminator is very famous anti-spyware software. It is used to destroy the lot of spyware in the system. But Microsoft's security application- windows Defender –detected spywareterminator.exe as Adware: Win32/Generic A. Then the spyware terminator venders reported this false positive and it has been removed from the malware database. Like this some situations the another security application warns the security utility as a virus.

**Monitoring the system**

To secure the system many users install Keyloggers. A specially the home users monitoring their children activities while they are using the Internet the parents install the Keyloggers in their systems. Or some companies want to monitor their employees they are also use remote keylogger. Keyloggers are used to read every keystroke of the user.

Fig. 3 shows sample format for how the data are recorded in the keylogger file. The file may contain the username and passwords and credit card number information, e-mail ids, phone numbers, account numbers, personal information and other sensitive data. They are lot of freeware also available in the market. Keyloggers has an option to send logging files to e-mail ids. If may it works as a hacking the information, the entire confidential data send to another person. That is, passwords, credit card numbers and other sensitive data. But still the user or secure system cannot identify the program hacking the data. Because

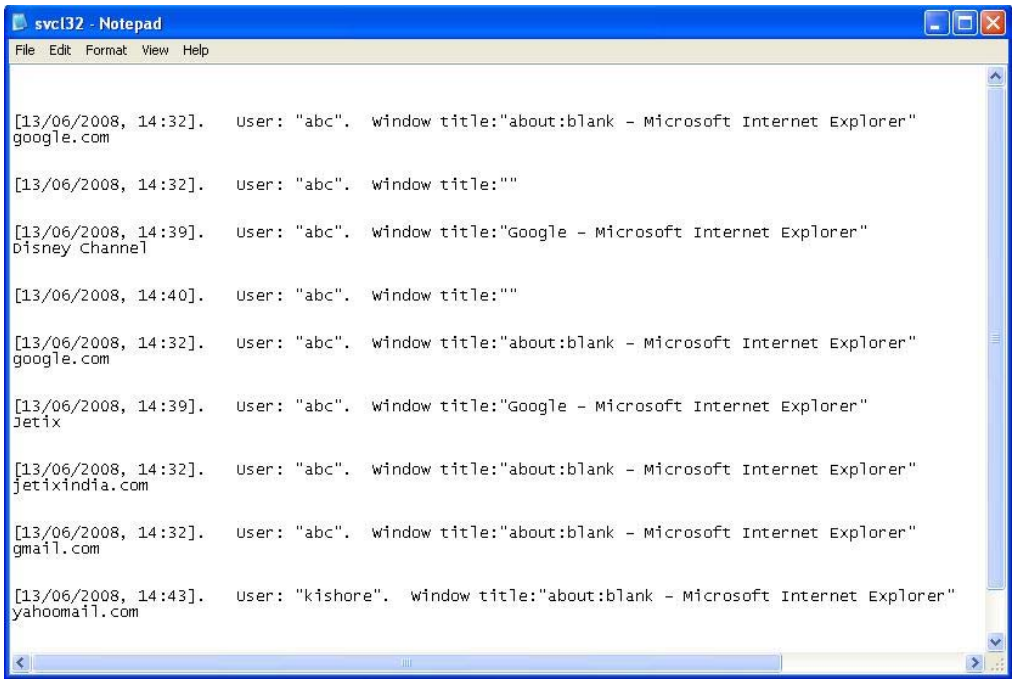


**Fig. 3**

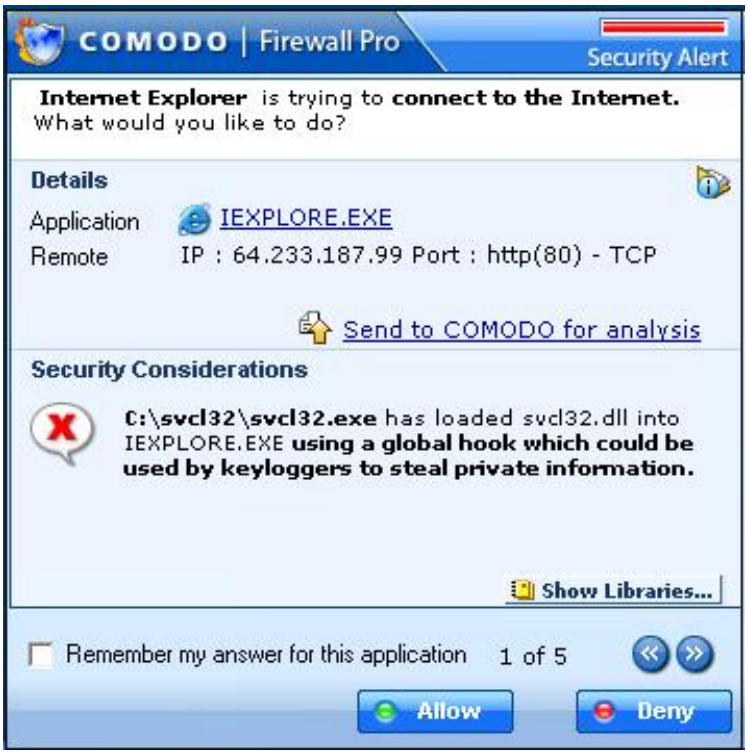
COMODO | Firewall Pro
Security Alert
Internet Explorer is trying to connect to the Internet.
What would you like to do?
Details
Application
IEXPLORE.EXE
Remote
IP : 64.233.187.99 Port : http(80) - TCP
Send to COMODO for analysis
Security Considerations
C:\svcl32\svcl32.exe has loaded svcl32.dll into IEXPLORE.EXE using a global hook which could be used by keyloggers to steal private information.
Show Libraries...
Remember my answer for this application
1 of 5
Allow
Deny

**Fig. 4**

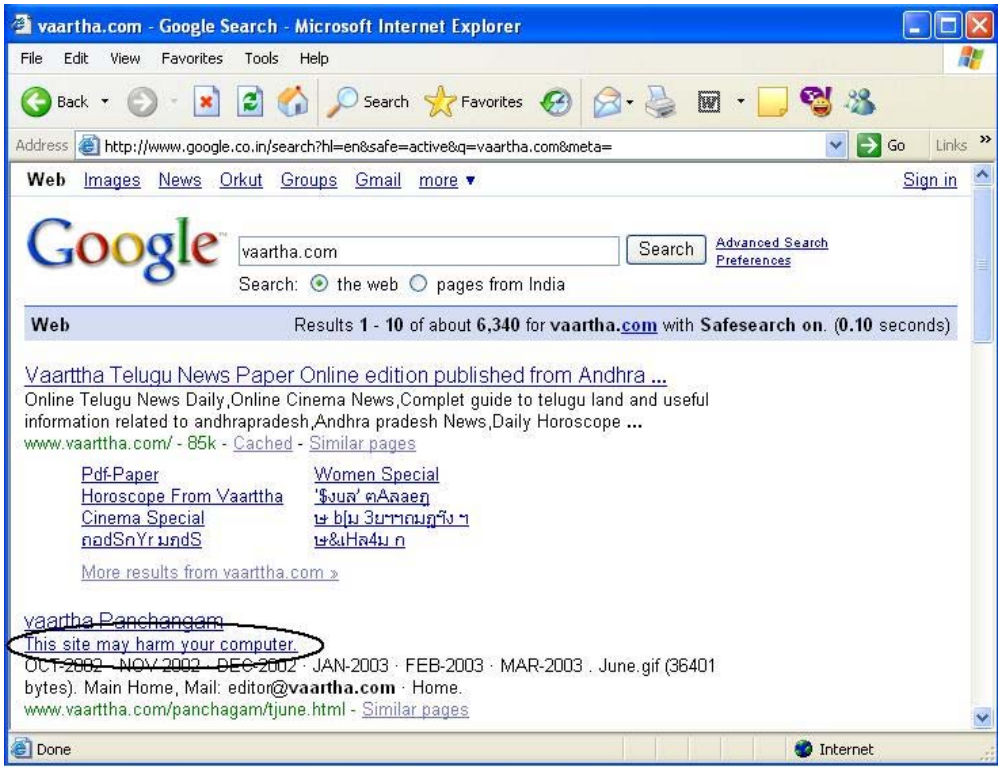
vaartha.com - Google Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.co.in/search?hl=en&safe=active&q=vaartha.com&meta=
Go Links
Web Images News Orkut Groups Gmail more
Sign in
Google
vaartha.com
Search
Advanced Search
Preferences
Search: the web pages from India
Web
Results 1 - 10 of about 6,340 for vaartha.com with Safesearch on. (0.10 seconds)
Vaarttha Telugu News Paper Online edition published from Andhra ...
Online Telugu News Daily,Online Cinema News,Complet guide to telugu land and useful information related to andhrapradesh,Andhra pradesh News,Daily Horoscope ...
www.vaarttha.com/ - 85k - Cached - Similar pages
Pdf-Paper
Horoscope From Vaarttha
Cinema Special
Women Special
More results from vaarttha.com »
vaartha Panchangam
This site may harm your computer.
OCT-2002 · NOV-2002 · DEC-2002 · JAN-2003 · FEB-2003 · MAR-2003 . June.gif (36401 bytes). Main Home, Mail: editor@vaartha.com · Home.
www.vaarttha.com/panchagam/tjune.html - Similar pages
Done
Internet

**Fig. 5**

when the program starts the system may warn about the software to the user. It shown in figure-4. But the users taught that this is only spy the data when keyboard are used and it used only for personal use. Therefore if the secure utility may warn about the keylogger software the main users simply allow that software for access.

**Misuse of the secure systems**

Many users are wanted to hide the system information and ip address. Using this ip address the other users can easily identify from where the user browsing and which websites they are browsing. For this reason or user want to do criminal activities like hack the information of the other user in and invisible mode, the user wants to hide the ip address. For this reason the software the user may install the hide ip address programs. But these programs may hack the ip address. Since using this ip address the hack users will do any illegal or criminal activities but problems are came to user.

**Unauthorized users are using the system**

The system user responsibility to only certain trusted people only access the system. Normally most of the people cannot give secure preference to other systems. When they are using the other system if the secure program warns about any threat other users cannot give any preference and the people allow the threat to the system therefore the system is infect by the threat. Therefore using human activities the secure utilities are failed to protect the system.

**Unsecured websites**

We have lot of security programs but most of the programs cannot protect the system while they are accessing any websites. If the user confused about the website. Then lot of search-engines provides the messages about un trusted sties. For example The google search-engine provides this facility for the net users. When the site is untrusted the google message that "This site may harm your computer".The Fig. 5 is shown the example for this situation.

**Suggested precautions**

***** The problems for failing the many security utilities cause the human activities. Because less system knowledge for the users. There fore the security utilities must work as a expert mode and it knows the every program at least mostly used programs and do not confusedly warn about the program.

* The users must update their secure programs. The users cannot neglect the updating of the system. The user must set the automatic option when they connect to Internet. And it is necessary to know if that software is perfectly working. The users also known the hardware capacity of their system. Since after some updating the software requires more capacity of the system, this situation the system may damage.

*The users only install the secure programs depend on user reviews and rating. And do not attract to the vendor's advertisements.

* When the users using Keyloggers the log files cannot send to any emails. That is, those are not accessed in the online.

*The system is used by sufficient knowledge users and whom the user trusts. There fore User may set passwords for accessing the system and some of the data files.

Finally when the use inter into any website or install any software the user must aware of these activities.

## CONCLUSION

Every hacker normally hack the information of the user when the people near to them or the people knowing by them etc. But when the user some time may enter into harmful coding websites or install harmful software's the hacker can easily identify their ip address and the user sensitive data then the hacker want to hack the sensitive information of the person.

There fore the secure program is strong to stop the threats enter into the system. And the program must be user-friendly. But still take all the precautions the security system programs are failed. Because at every second, worldwide lot of hackers

want to hack the systems. Therefore at every time the hackers create lot of threats for destroy system user activities or stealing the user information.

The hacker every time to design the threats without identify by the security programs.

Therefore the security program at any time failed by the new threat. So, the user must update the software every day. For this reason the users not satisfied or trust on only security program there fore the users every time searching for good network security programs for secure the system.

**APPENDIX**

| Topics | Page Numbers |
|---|---|
| Anti-Spam | 3 |
| Anti-Spy ware | 3, 4 |
| Anti-Virus | 2, 3 |
| Conclusion | 5 |
| Firewalls | 3 |
| IP Address | 4 |
| Key loggers | 1, 4, 5 |
| Precautions | 5 |
| Threats | 1, 3, 4 |

## REFERENCES

1. WILLIAM Stallings "Network Security Essentials applications and standards", Third Edition, PHI.
2. Applied Operating System Concepts – Avi Silberschatz, Peter Galvin, Grey Gagne, Sixth Edition.
3. http://www.webopedia.com
4. http://www.personalfirewall.comodo.com
5. http://en.wikipedia.org
6. http://www.spywareterminator.com
7. http://free.grisoft.com