ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

Detection and Prevention of Passive Attacks in Network Security

Jatinder Teji, Rimmy Chuchra, Sonam mahajan, Manpreet Kaur Gill, Manju Dandi

Abstract: ***This paper describes how to detect passive attack and after that provide prevention from passive attacks. For detection of passive attacks we use the concept of key loggers and the concept of registry files. For prevention from passive attacks here we use the concept of virtual keyboards and concept of NAC during online transmission of data. The major function of keyloggers is to record all inputs, hide itself and monitor applications. Here, we will also discuss the behavior and types of keyloggers.Basically the concept of keystrokes used by virtual keyboards. In this paper, we will combine network security with unethical hacking. The logical significance to study the concept of unethical hacking with passive attacks is passive foot printing is the first step towards it. The major benefit to combine these concepts to check the behavior of the network either it is secure or not during data transmission.***

Index Terms: **Key loggers, CAPTCHA, network security, registry files, unethical hacking, virtual keyboards, NAC (Network access control).**

I. INTRODUCTION

Network security measures are needed to protect data during their transmission. It basically interconnects their data processing equipment with a collection of interconnected networks. Such kind of collection is often referred to as an internet for this we use the term "Internet security". Here, our major goal is to provide "information security" of data during online or offline mode and to protect data from the "black hat hacker" during online data transfer. There are several types of attacks will occur on the network like active attacks or passive attacks. There are four types of active attacks are available like replay, masquerade and modification of messages and denial of service etc. Repetition of same files in a system, alteration or modification of files and new folder etc are the symptoms of active attacks done by the hackers. We can also say that active attackers always show their physical presence. Similarly there are three types of passive attacks are available like traffic analysis and release of message contents. In case of release of message contents third party say user 'C'(is invisible from user 'A' and 'B') read messages of user 'A' and user 'B' Moreover passive attackers does not show their physical presence but effects on the network and steal information. There are many more practical applications are related to this concept is used in this real world like to provide security of personal data of any organization which can only transferred in online mode, whether in every domain like in finance, marketing,HR ,economics etc.

Unethical hacking is basically illegal hacking which is not performed with the permission of any organization. The goal of unethical hacking is to gain access of any organization and give permission to use information and you can steal or modify information and also misuse that important information of the organization. There are three broad categories of hackers are available which are listed below:

a) White hat hackers: They perform ethical hacking and used by the security professionals for improve the level of security.

b) Black hat hackers: They perform unethical hacking. A type of criminal hackers/crackers that use their skills and knowledge for illegal or malicious purpose.

c) Gray hat hackers: These are sometimes behaving like a legal hacker used in ethical hacking and other times behave like an illegal hacker used in unethical hacking. In other words, we can say that gray hat hackers are the combination of white hat hackers and black hat hackers.

Here, we use a type of "black hat hackers". They may be "CRACKERS" are used to perform unethical hacking where are "HACKERS" performing ethical hacking. All hackers are crackers but all crackers are not hackers.

"HACKER IS A BUILDER WHERE CRACKER IS A BREAKER".

Any hacker can entered into the network at any time and performs hacking either manually or with the help of hacking automated software. There are various symptoms are used to show the presence of hackers in the network like system speed may be slow and delay possible that automatically affects on the performance. In general our daily life most common methods for the detection of presence of hackers by using two methods like with the help of firewalls and by using the concept of "Port scanning". More than 70 % hacking is done through

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

the firewalls we can protect this by installing various anti-virus software's. In the concept of "port scanning" server check the service going on the specific port. If server is unaware of that specific IP address and check from where IP address come either come from legal organization or come from the hacker side. We can also detect the behavior of the hacker with the "spy ware" just the listen the conversation and steal all important data.

In this research paper, we are merging two broader areas network security with unethical hacking. We can *detect* the passive attacks by using the concept of key loggers and registry files in the system. After the detection of passive attacks we must have to *prevent* the passive attacks by using the concept of network access control (NAC) and the concept of virtual keyboards.

II. OUR CONTRIBUTION

In this paper, we proposed a "hybrid approach" that is unethical hacking with network security. By using these both concepts collectively we can easily identify the passive attacks done over the system either in online mode or in offline mode.

Step-1) Identify passive attacks.
a) By using the concept of Key loggers.
b) By using registry files in the system.
Step-2) Prevent from passive attacks.
a) By using the concept of virtual keyboards.
b) By using the concept of NAC in online mode.

In first step, we are considering example of key loggers attacks that is also a one way of passive attack. Key logger is a major thread to business and personal activities, email, chat etc. In this paper we present the detection and prevention from the key loggers attack.
When we press any key from the ordinary keyboard then all pressed keys are auto-saved and key logger steal all these pressed key details information and perform "keystroke". Where keystroke per minutes are used to measure the typing speed instead of words per minute (WPM). In this way key loggers can easily detect all the meaningful information of the user through the system.
To provide protection from the passive attacks we use virtual keyboard rather than ordinary keyboard. Virtual keyboard shows touching of the image of a key generates a unique electronic signal corresponding to a key image. There are number of reasons to used virtual keyboards rather than ordinary keyboard which are discussed below:
a) Eliminates the chance of the breakage.
b) No wires and buttons.
c) It is much compatible with the smart phones and PDA (Personnel digital assistant).
e) Smaller as well as faster.

Two major advantages of virtual keyboards are projected on any surface like air and high battery life standard coin sized standard. The function of virtual keyboards is to detect the movements when fingure is pressed down. Those movements are measured and device accurately determine the intended keystrokes and translate them into text and additionally we must have to provide encryption by using certain encryption algorithms like DES(Digital encryption standard) and AES(Advanced encryption standard) algorithm so that keystrokes can be stored in encoded from called "cipher text" where breakage of DES and AES algorithms are too hard almost impossible because of size of keys used in these are too large and used various combination of keys that takes too much time to break but no guarantee. By providing encryption on data during input especially through virtual keyboards we can easily protect our information from the key loggers. In other word, we can also say that choice of keyboard becomes too necessary while providing prevention from passive attacks. It uses light to project a full size computer keyboard onto almost any surface and disappears when not in used. In this way we can say it allows users to leave laptop at home.

Other alternative method to prevent form passive attacks is using the concept of NAC (Network Access Control). Basically NAC helps/attempts to fix this problem by ensuring that every device is connected are trusty before full network connectivity is delivered. Before using NAC registration on the network is a mandatory step. After the confirmation of the registration network will automatically generate an "ID" after Sign In by this ID

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

user can only access the network. If any hacker or attacker want to entered into the network then he/she must complete the first step of registration on the time of registration in NAC here party is not trustworthy then not possible to entered into the network and hence registration will be failed. In this way we can easily prevent our network through the untrusted party. Whenever any user or device entered into the network then the concept of NAC verifies the party is trustworthy or not verifies the registered ID. If not then we can easily detect). It is a type of passive attack that helps to prevent data from the third party. This can be shown in figure 1 given in research design.

Most important reason for detection of passive attacks is to use information and learn information from the system *without injecting traffic*.

With the help of "registry files" we can also detect the passive attacks. Registry files further consist of two types of files.
a) DLL files (from their keystrokes read all data).
b) Txt.exe (these all included in DLL files).

Registry files further consists of number of log files in the system.Similarly "Log files" store all type of information used in login or logout time.

III. RESEARCH DESIGN

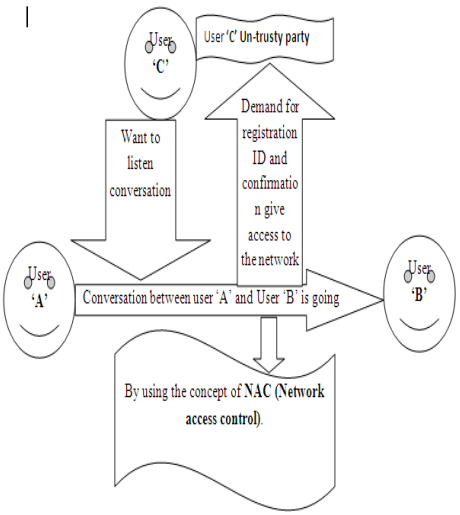

Fig 1. Proposed design to provide prevention from passive attacks.

Description: In this figure 1 the conversation between user 'A' and user 'B' is going on.Instantly user 'C' who is untrusty party want to listen the conversation of user 'A' and user 'B' but network will not allow access this they must first have to register in the network with specific details after the confirmation of registration Id any third person will access the network by using NAC(Network access control) method.When registration ID of specific network will be confirmed then it alotted a security certificate with encrypted digital signature with proper time and date.If in future any fake or untrusty user will come and want to enter into the network then must follows this procedure, if that specific party will entered fake information it will not received. (like PAN number of the user must be required during confirmation of the registration ID obviously it will be orignal. Every user has its own PAN number) then ultimately Id will not be generated by the network. In this way we can say that if any fake or un-trusty user will not entered into the network without registrationID and it will not be capable to generates security certificates and hence can not access your network.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 6, November 2013

IV. CONCLUSION

In this research paper, we have discussed a "hybrid approach" that merges two separate broader areas unethical hacking and network security. It also tells how black hat hacker applies unethical hacking to steal information in online and offline mode and also provide prevention during online mode by using the concept of NAC. There are many more practical applications are related to this concept is used in this real world like to provide security of personal data of any organization which can only transferred in online mode, whether in every domain like in finance, marketing, HR ,economics etc.

V. FUTURE SCOPE

In future, this concept of CAPTCHA will be used for the screen capturing rather than key loggers. Key loggers basically used for password hacking and online financial theft. But it has one major drawback it slow down the speed of the system while screen capturing ultimately increase the risk of detection. Screen capturing also provides voice and video interactions for ensuring the exact captured information. Screen capturing will be provided with the help of CAPTCHA not by the automated software. It is a type of challenge/response test to ensure that response is only generated by humans not by computer. So, chances to create disturbances and steal information by the black hat hackers will be ultimately decreases. In this way CAPTCHA automatically provides "Prevention" from an automated software or boots for performing action on the behalf of actual humans. For example during Sign Up we experience with CAPTCHA where text/numeric is put by the legitimate user even not by the automated software and response will be generated by the humans.

REFERENCES

[1] S. Sagiroglu and G. Camber, "Key loggers," IEEE Technology and Society Magazine, vol. 28, no. 3, pp. 10 –17, fall 2009.

[2] T. Olzak, "Keystroke logging (key logging)," Adventures in Security, April 2008 (accessed May 8, 2010), http://adventuresinsecurity.com/images/Keystroke_Logging.pdf.

[3] S. Shah, "Browser exploits - attacks and defense," London, 2008 (accessed May 8, 2010), http://eusecwest.com/esw08/esw08- shah.pdf.

[4] B. Whitty, "The ethics of key loggers," Article on Technibble.com, June 2007 (accessed May 8, 2010), http://www.technibble.com/ the-ethics-of-key-loggers/.

[5] Adeyinka .O, "Internet attack methods and internet security technology, "Modeling and simulation", 2008. AICMS 08. Second Asia International conference on vol., no. , pp 77-82, 13-15 May 2011.

[6] Marin, G.A, "Network security basics", "Security & privacy, IEEE, vol.3, no.6, pp.68-72, nov-dec.2008.

[7] Curtin, M. "Introduction to network security", http://www..interhack.net/pubs/network security.

[8] "Improving security", http://www.cert.org/tech_tips,2009.

[9] "Security Overview", www.redhat.com/docs/manuals/ enterprise/RHEL-4-Mannual/security-guide/ch-sgs-ov.html.

[10] www.scribd.com/doc/128633322/virtual.keyboard.

AUTHOR BIOGRAPHY

Er.Jtinder Kumar Teji : He is working as an Assistant Professor in Sai institutes of engg. And technology, Mannawala(Amritsar) and completed her M.Tech from MMU, Kurukshetra. He published many papers in international journals and national conferences. His areas of interests are Digital image processing, hacking and databases.

Er. Rimmy Chuchra: She is working as an Assistant Professor in Sai institutes of engg. And technology, Mannawala(Amritsar) and completed her M.Tech from Lovely Professional University,Jalandhar. She published many papers in international journals and conferences. Her areas of interst are data mining, cloud computing and network security.