INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

IMPLEMENTATION OF ACTIVE WARDEN DEFENCE MODEL FOR STORAGE COVERT CHANNELS

Dhananjay M. Dakhane[1] and Prashant R. Deshmukh[2]
[1]Department of CSE Sipna College of Engineering and Technology, Amravati(MS), India
[2]Department of Electronics Egineering Dr. P. D. Polytechnic, Amravati(MS), India
ddakhane@gmail.com

Abstract:
Covert channel is a transfer of unintended information. It allows an attacker to send and receive the secrete message without being identified or detected by the network administrator. It is observed that, covert channels can easily implemented by embedding the covert message in the various header fields seemingly filled with "Random" data. Network covert channel generally use for leak the information by violating the security policies. These channels can be created as a part of Storage covert channel and Timing covert channel. However there is always some possibility of these covert channels being identified depending on their behaviour. In this paper, we propose, an active warden defence model, which normalizes all incoming and outgoing network traffic and eliminating all possible storage based covert channels. It is specially design for TCP sequence number and IP Identification field, because these field has a maximum capacity vehicle for storage based covert channel. Our experimental result shows that propose model eliminates covert communication up to 99%, and overt communication is as intact.

Keywords: Active Warden, Covert channel, IP Identification, Network Covert channel, TCP Sequence Number, Traffic Normalization.

Introduction:

Definition of covert channel defined by DOD, it is a communication channel that can be exploited by a process to transfer information in a manner that violates a systems security policy [1]. Covert channels used in TCP/IP protocols is a new challenge for network security as well as organization security policies. These types of methodologies required to change communication medium unconventionally [2]. Covert channels mainly classified in two: covert storage and covert timing channels [3][4].

For any organization security of their information is crucial. If someone from the organization internally leaking the information to the third party, it will be a huge financial loss. Everybody worried about the security of their information. The most probable solution will be an active warden. An active warden is specialized network security systems which is design in order filter miscellaneous anomalies present in the network traffic. An active warden is usually located at the gateway system of the network through which all the traffic in the network passes through. The security improvements can be achieved in the system by enhancing the functional capabilities of the gateway system.

Literature Survey:

Passive wardens only observe information flows and try to detect the steganographic or covert elements, embedded content and try to prove that a third party is involved in the communication. Active wardens have the ability to modify the information flows [5]. In a malicious variant of an active warden, the active warden does not only manipulate steganographic content but does also introduce new bogus messages into the covert communication [6].

In the literature of information hiding, it is mention the difference between active and passive wardens [7] which can be seen as the adversaries for the area of covert channels. A traffic normaliser is a network gateway with filtering capabilities that enhances the capabilities of a simple firewall. In the literature, a traffic normaliser is sometimes also referred to as a packet scrubber or as a firewall with scrubbing functionality [8]. While a plain firewall can block and forward traffic, normalisers can be seen as advanced firewalls/intrusion prevention systems capable to modify traffic [9]. Thus, a traffic normaliser can remove malicious/steganographic elements of network traffic and can forward the remaining data. For instance, a normaliser can clear a specific bit used for information hiding or can unify a field in network protocol headers [10]. Thus traffic normaliser can be considered as a active warden In Active Warden [11], Fisk et al. gave the concept of Minimal Requisite Fidelity (MRF). MRF is a measure of signal fidelity which is required for an acceptable communication channel and prevents covert communication without disturbing the overt communication. Structured carriers with well defined semantics such as TCP and IP are defined for active warden with respect to Minimal Requisite Fidelity, which is acceptable by sender and receiver. After intercepting the communication between two processes, Active warden applies a set of rules to prevent transmission of covert data.

Proposed Active Warden Defence Model

Our first objective while designing an active warden defence model, it should be capable of eliminating or blocking storage covert channels which are exploited by manipulating one of the TCP or IP header fields or even both in order to communicate covertly. The proposed active warden defence model use the technique called as protocol normalization in order to eliminate the potential covert channels.

The second objective is, while eliminating the covert communication, the overt traffic in the network will consume it fidelity as per the concept of DMRF (Definite Minimal Requisite Fidelity). This model implements an algorithm which does the protocol normalization on Transport, Internet, Network layers of the TCP/IP and leaving the application layer data untouched. So as consequences of this, all the semantics of the structured carriers get normalized at these layers. This scenario is shown in Fig. 1.

An active warden modifies some contents in the network traffic in order to eliminate or identify the vulnerabilities in the network traffic [12]. In the proposed model implementation it will normalize the incoming and outgoing network traffic in order to eliminate or block the possible storage based covert channels [13] [14] in the network.

Active Warden Design Module

The block diagram of the proposed active warden model is shown in fig. - 2. The protocol normalization is vendor or implementation specific technique.

In this proposed model, the protocol normalization is being used for our implementation specific way and it implemented with following four components:

1. NetFilter Hook Module
2. Netlink Kernel IPC Module
3. Netlink User IPC Module
4. JNI for Bridging Java and C Modules.

The packet normalization is used for the purpose of eliminating potential covert channels present in the network [15]. The netfilter module is used to hook all the incoming as well as outgoing packets. The gateway system is configured in such a way that, all the network traffic will always pass through the gateway or active warden model.

a) NetFilter Hook Module:

The netfilter module is being used in order to hook all the incoming as well as outgoing packets, whenever an incoming packet arrives at active warden model. It hooked by the module and it's corresponding destination port and destination IP is changed forcing the packet to redirect at the gateway system. The track of all such a intercepted packets are being kept in kernel level table which is implemented as linked list in the system.

b) Netlink Kernel IPC Module:

The netlink kernel module is used in order send the packet specific data which is referred to be meta-data which is then send to the application layer.

c) Netlink User IPC Module:

The netlink kernel user space module is used to receive the packet level metadata information send from the netlink kernel module and then it makes the entry in the corresponding hash map respectively.

d) JNI for Bridging Java and C Modules:

The Java Native Interface here is used in order to call java application which does the work of payload exchanges between two end systems from the C netlink user program.

Experimental Results

The experimental results are taken with the various tests are conducted in the presence of our active warden defence model.

a) Active Warden Correctness Test

This test is conducted to check correctness of active warden defence model. In this test the overt communication traffic is observed in the presence of active warden model. A 1024 bytes of data file is send as a normal overt communication and it observed at receiver side. The result of our Java application after comparing byte by byte of both files is shown in Table -1.

b) Active Warden Covert Channel Test

This experiment is conducted to test the effectiveness against the covert channels attacks. The percentage of covert blocking by proposed active warden model is measured for various test in network environment. The effectiveness of active warden model is tested against our proposed covert reference models. For all tests, the size of covert message is 1024 bytes.

TCP SQN 32-Bit Reference Model Test

In this test, covert sender is transmitting 32 bit covert data per packet, using TCP-SQN field as the reference. The covert message size 1024 bytes is considered. Test Result for this model is show in Table – 2

Table – 1 Active Warden Correctness Test

Test No	Total Bytes	Covertly Received Bytes	Overt Blocking	Overt Correctness
1	1024	1024	0%	100%
2	1024	1024	0%	100%
3	1024	1024	0%	100%
4	1024	1024	0%	100%
5	1024	1024	0%	100%

Table – 2 TCP SQN 32-Bit Reference Model Test

Test No	Byte Blocked	Byte passed	Blocking Percentage
1	1016	8	99.21 %
2	1020	4	99.60 %
3	1013	11	98.92 %
4	1023	1	99.90 %
5	1023	1	99.90 %

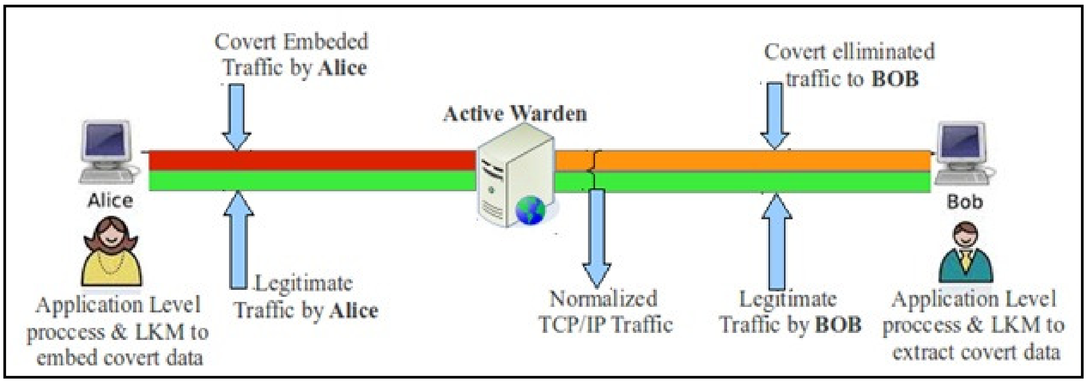
Covert Embeded Traffic by Alice
Covert elliminated traffic to BOB
Active Warden
Alice
Bob
Application Level proccess & LKM to embed covert data
Legitimate Traffic by Alice
Normalized TCP/IP Traffic
Legitimate Traffic by BOB
Application Level proccess & LKM to extract covert data

Figure 1 Active Warden Defence Model

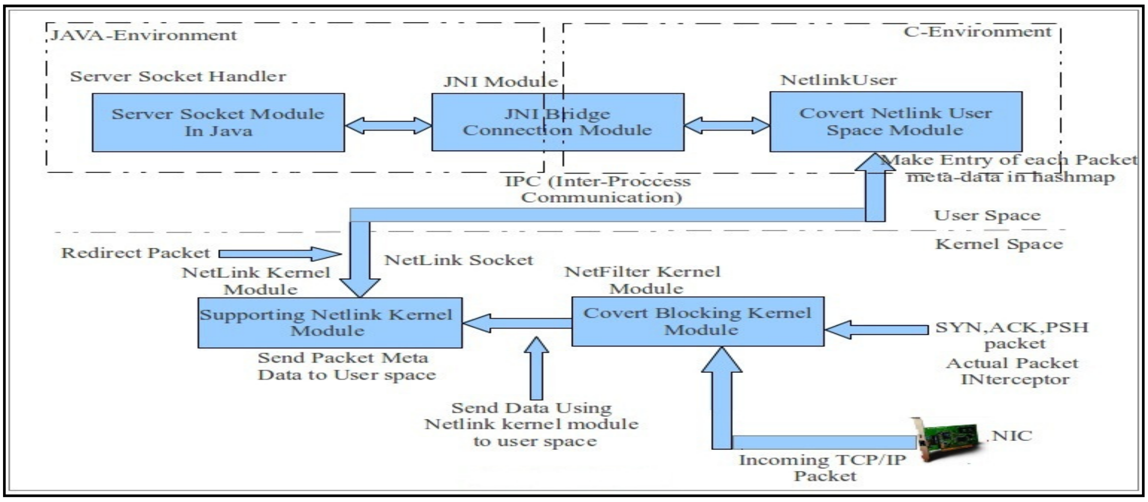
JAVA-Environment
C-Environment
Server Socket Handler
JNI Module
NetlinkUser
Server Socket Module In Java
JNI Bridge Connection Module
Covert Netlink User Space Module
Make Entry of each Packet meta-data in hashmap
IPC (Inter-Proccess Communication)
User Space
Kernel Space
Redirect Packet
NetLink Kernel Module
NetLink Socket
NetFilter Kernel Module
Supporting Netlink Kernel Module
Covert Blocking Kernel Module
SYN,ACK,PSH packet Actual Packet INterceptor
Send Packet Meta Data to User space
Send Data Using Netlink kernel module to user space
NIC
Incoming TCP/IP Packet

Figure 2 Active Warden Design Module

Conclusion

An active warden normalizes the individual packet header semantics in order to remove or eliminate any possible anomaly that can exploited through the under- lying network traffic. The impact of traffic normalization in the context of active warden system affects the overall behaviour of network. The results indicates that proposed an active warden model is capable of eliminating all possible storage based covert channels.

References

[1] U.S. Department of Defence. Trusted computer system evaluation criteria, 1985.

[2] R. J. Anderson and F. A. P. Petitcolas, “On the limits of steganography,” IEEE J. Sel. Area Commun., vol. 16, no. 4, pp. 474–481, May1998.

[3] S. Attallah, Trusted Computer System Evaluation Criteria, Tech. Rep. DOD 5200. 28-STD, 1985

[4] R.A. Kemmerer. A practical approach to identifying storage and timing channels: Twenty

years later. In Computer Security Applications Conference, 2002. Proceedings. 18th Annual, pages 109–118, 2002.

[5] B. Pfitzmann. Information hiding terminology - results of an informal plenary meeting and additional proposals. In Proc. First International Workshop on Information Hiding, volume 1174 of LNCS, pages 347– 350. Springer, 1996.

[6] S. Craver. On public-key steganography in the presence of an active warden. In Proc. Information Hiding, volume 1525 of LNCS, pages 355–368. Springer, 1998.

[7] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. Information hiding – a survey. Proc. IEEE, 87(7):1062–1078, 1999.

[8] K. Borders and A. Prakash. Quantifying information leaks in outbound web traffic. In Proc. 30th IEEE Symposium on Security and Privacy, pages 129–140, 2009.

[9] G.R. Malan, D. Watson, F. Jahanian, and P. Howell. Transport and application protocol scrubbing. In Proc. 19th Annual Joint Conference IEEE Computer and Communications Societies (INFOCOM 2000), pages 1381–1390, 2000.

[10] M. Handley, V. Paxson, and C. Kreibich. Network intrusion detection:Evasion, traffic normalization, and end-to-end protocol semantics. In Proc. 10th USENIX Security Symposium, volume 10, pages 115–131, 2001.

[11] Gina Fisk, Mike Fisk, Christos Papadopoulos, and Joshua Neil. Eliminating Steganography in Internet Traffic with Active Wardens. In IH '02: Revised Papers from the 5th International Workshop on Information Hiding, pages 18-35, London, UK, 2003. Springer-Verlag.

[12] Hammouda, S.; Maalej, L.; Trabelsi, Z., "Towards Optimized TCPIP Covert Channels Detection, IDS and Firewall Integration, New Technologies, Mobility and Security," NTMS, vol.1, no.5, pp. 5-7 November 2008.

[13] R. A. Kemmerer, "A Practical Approach to Identifying Storage and Timing Channels," Proceedings of IEEE Symposium on Security and Privacy, April 1982

[14] C. H. Rowland, "Covert channels in the TCP/IP protocol suite," Technical Report 5, Peer Reviewed Journal on the Internet, July 1997.

[15] Zanders S, Armitage G, Branch P, "Covert channels and countermeasures in computer network protocols," IEEE Communications Magazines, vol. 45, no. 12, 2007.