A NEW APPROACH FOR DETECTING MALICIOUS CHANNELS IN THE NETWORKS

Shaik Rafi[1], Boppudi Swanth[2], Betam Suresh[3]

[1]*M.Tech(CSE), Vikas Group of Institutions (Formerly Known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada, A.P, (India)*

[2] *Assistant Professor, Department Of CSE,Vikas Group Of Institutions, Nunna, Vijayawada, (India)*

[3] *HOD, Vikas Group of Institutions (Formerly Known As Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada, A.P, (India)*

ABSTRACT

The covert channels via a broadly used TCP/IP protocol have turn into new challenging issues for the network securities. In the proposed paper, we analyses information's hiding into the TCP/IP protocol and then propose the new useful method to identify the existence of the hidden information's in the TCP primary series number (ISNs), that is finally known as the one of most complicated covert channel to be detect. Proposed method is using a phase space reconstructions to generate a processing space that is called reconstructed phase spaces, where the statistical method is projected for the detecting of covert channel in a TCP ISN. Based on this model, the classification algorithm has been developed for identifying the existence for information hidden in the ISN. Simulation result has demonstrated that the proposed one detection method outperform state of an art system in the term of high detection accurateness and really reduced the computational complexities. In the place of an offline processing as state of the arts does, the new scheme can be use for the online detections.

I. EXISTING SYSTEM

A **S**TEGANOGRAPY is an art and a science for writing the hidden messages to the medium cover in such the way that, no one, apart from a sender and a intended receiver, suspect for the reality of a message. The Most commonly available application of the Stegnography is dedicated to the multimedia's application in that hidden data's are distributed via the file of a sound, an image and a video. And Stegnography can also be useful in digital watermarking in the context of protecting the copyright in varieties of the digital audios, videos and the software's entity. If it is well applied, then it can provide a means of authentications, and certification validations, and a standard for the non repudiations. For hiding the data's at the network levels such as the protocol is relatively latest, but now it becomes the crucial issue for the network securities. All the information's hiding method which can be used for exchanging steganograms in the telecommunications network can also be classify under a common term of the network Stegnography. Contrary to these typical steganographics methods that make use of a digital media (image, audios and video's file) as the cover for the hidden data's, networks Stegnography uses communications protocols control element and the basic intrinsic functionalities. As the result, such kinds of the methods are not easy to identify and remove. The typical networks Stegnography method or the network based coverts channel manipulates the certain property for communication means in the sudden or unconventional ways in the order to transmitting the secret information all through a way without drawing the attentions by anyone other than that entity operating covert channels. The covert channel is described as the variant of the information's hiding research areas. In the proposed papers, we treat's it as a form of the Stegnography. And traditionally, the covert channels are also classified into the storage

space and the timing channel. The covert storage space channel can also be explained as the writing of the hidden information's into the storage space locations (it's not specifically meant for a usual communications) by transmitting parties, and subsequent recovery of a hidden information's by receiving the party. In the contrast, communications into the covert time channels happens when the communicating entities signal information's to the other communication's entities by modulating the own use of the systems resource in such the way's so that the changes in the response times got by second communication entities would then provides the information. The network based covert channel that uses the protocol as a carriers for hiding the secret facts can considered the covert storage space channel. And hiding the data's at the network levels such as a protocol was initially launched by Girling and Wolf. The Girling noticed that there are three coverts channel in the typical networks via the *Address Fields, length of the data blocks*, and *timing between the consecutive transmissions*. A wolf there showed a potentials unused bandwidth in normally used LAN protocol for example IEEE 802.2, and 802.3, and 802.4, and 802.5 that might be vulnerable as the covert channels. As all covert channel stays in the LANs and they cannot go across Internet, and it did not raised much of the attention to public, and in many of the circumstance, The physical securities may be the more practical ways for protecting the networks against these covert channel in the LANs than use of the encryption or the complex mechanism.

II. DISADVANTAGES

1) Many of the application of covert channel are of malicious or an unwanted nature, and hence pose the very serious threat for network securities.

2) The ITCP/IP based covert channel (or a TCP/IP Stegnography) exploits fact that some of the header field could also be alter for carrying the information's in a transit without impacting the ordinary communication.

III. PROPOSED SYSTEM

Use of the pseudo random numbers generator (PRNGs) has been broadly spread when producing the ISNs. The PRNGs generates the sequences of all numbers which approximate the property of the random numbers. Therefore, sequence is not really random. Randomness of the ISNs use to make attacker very hard to predict those number; the idea behind that is not to use truly the random numbers for ISNs that lies in that if the connections arrive, randomness of the ISNs would build it tentative that coming series numbers would be all different from the earlier incarnation. For the IP IDs, as uniqueness inside the given time windows ensure that fragment of the different packet aren't reassembled in single packet on receiving hosts, real random numbers should not get used into IP IDs. PRNG that is used by Windows operating systems is most generally used PRNGs. Pseudo randomness of output of the generator is very crucial for securities for almost all application that is running into Windows. Though, the accurate algorithm was never been published. PRNG is initially modeled as the functions whose inputs are short random seeds, and output is also indistinguishable from the all truly random bit. The Implementation of pseudo random numbers generator is often uses the state whose first value is random seeds. State is updated by the algorithms that change state and output of pseudo random bit, and then implement the deterministic functions of given states of generator. The Herring noticed that a pseudo random numbers generator is resultant from the deterministic chaotic systems and then made some connections between the chaos and the pseudo random numbers generator. The Gleick in his world popular book written on chaos, clarify all views of the several researchers:

- Complicated periodic attracting are orbits of the certain dynamic systems,
- Actually the random recurrent behaviors in the simple deterministic systems,

- And Irregular and unpredictable behaviors of the deterministic and nonlinear dynamic systems

Then author analyzed the Bernoulli algorithms and then pointed out all pseudo random numbers generator that are shifts onto finite precisions, and exhibit a chaotic behavior. For analyzing the chaotic or a nonlinear behavior, we have to turn to the phase space of reconstruction methods, which is the very handy chaotic or nonlinear signals processing techniques. The Zalewski has first used the method for building the spoofing sets in the predicting ISNs created by the Windows 2000. Several pitfalls of Windows PRNG were then revealed. In the proposed paper, the phase space for reconstruction method is used for creating the processing space's where the statistical models are further projected to identify covert channel. For this section, the method called a phase space reconstruction and finally how it can be reconstructed the time series in the multi-dimensional phase of space to representing underlying dynamics first reviewed. Statistical feature models are projected based on data sets that is formed by the reconstructing phase space's input sequence ISNs. The classifier based onto the projected statistical feature models is presented.

IV. ADVANTAGES

1) There is some scheme that is developed for hiding the information in the TCP/IP header, from them, informations hidden in the TCP ISN (the Initial Sequence Numbers) field and the IP ID (a Identifier) fields are most difficult one to be discovered.

2) In the proposed paper, we analyses all the possible coverts channels in the TCP/IP protocol and then offer a new resourceful schemes called the Phase Reconstruction Methods (PRMs) for identifying a covert channel in the TCP ISN and the IP Identifications fields.

V. RELATED WORK

Covert TCPs proposed by the Rowland is completely considered as the practical step forward in the encoding information's in TCP ISN fields and IPs identifications field as others methods stay in that theory level. Basis of a proposed data's embedding is relies on an encoding ASCII value in range of 0–127 in the ISN field or the IP ID fields. By using that method it's feasible to pass data's between the hosts in a packet which appears to be a initial connections request. In this experiment, steganographics ISNs are finally generated by using this method. Normal TCP/IP packets are then collected by Win Dump. Filter added to the Win Dump, and then could get the initial packet with a SYNs sets to the 1. After gathering TCP/IP packet, ISNs will be extracted from this packet. In the very first experiments, Data's Set1 consist of a 745 common ISNs—that are from a 745 TCP connection, and 350 ISN are then used for training models; and rest of them is used for testing. Number of the stego ISN generated by the Covert TCPs is totally 2000. All the data get collected based on the Windows XP SP3 (operating system), the given models needs to be train just once only by half of Data Set1 so it could be used in following test. As per the book, which is published by Microsoft's, Windows PRNG was then first launched in Windows 95 and was embedded in all the Windows operating systems such as a Windows XP or a Windows 2000 and in their entire variant. Design of the Windows PRNG has not been changed between different level versions of operating systems. And these indicate that the proposed models could be used in the other versions of the Windows operating systems. A 2000 abnormal ISN is applied for each of the testing. We finally compared the results with that by using the SVM that is proposed by in the term of numbers for feature used, correctness and the complexity as shown in the Table V.

TABLE V

Case	Number of features	TC (Total Correctness)	Training data (packets)
PRM	1	100%	350
SVM	1	92%	10000

The table V displays the proposed PRM outperform that is the Sohn's SVM methods in all fields, and most significant, we believe the actuality that the ISNs demonstrate some structure for avoid getting leftover packet from the past connections. Therefore, computational complications are reduced very much and proposed classifier is a lot easier than the SVM. In the Sohn's SVM methods, polynomial kernels are used; if the linear kernels are used, final accurateness achieved will be decreased to an 87.9%. Authors increased numbers of features to the three, and then total accuracy could be increased to the 99%. Though, these further increases computational complexities as the three field—a *Sequence Numbers* field, the TCP control *Flag* and the TCP *Checksum* field will get extracted from each of the TCP/IP packet as the features to be used into SVM. Computational complexities of the SVMs in the training are evaluated as, that include resolving the convex optimization difficulty. In the given PRM, one field—that is ISN field will be used for model constructions and model constructions does not include solving the convex optimization work. Computational complexities are evaluated as. By the use of third orders feature, we can then clearly recognize a normal and a stego ISNs with the accuracy rate of 100%. The proposed model constructions need to be done only once for the specific operating systems and training data's used is approximately 350 normal ISNs in the experiment while 10000 is being used in the Sohn's methods in that 5000 for the normal ISNs and a 5000 for the stego ISNs, that is then considered as impractical. And it is known that the networks stego analysis is not like an image stego analysis that could be carried out as offline. Covert channels need to get detected by online because the header information's (for example TCP header) will be taken off as packets reached to its closing destination. It is also possible that secret message's has been passed earlier than gathering these stego based packet for that training is over.

VI. CONCLUSION

The large amount of the data transmitted over the Internet by using the TCP/IP protocol makes it best as a carrier in the Stegnography. The attack based on the covert channel becomes the potential threats to Internet. The covert channel based onto reserved field, unused grouping of the flag fields of a TCP/IP header, or alteration of some of the header fields can also be simply noticed or eliminated. Detecting the covert channel into the TCP ISN fields is known as the one of most problematic covert channel to get detected. Before this not many research work in this context has appeared in literature. The Sohn and the Moon have given to use a SVM to detect the covert channel in ISN fields. Though, their proposed methods are complicated and also time consuming, so hence are not at all appropriate for the network's online uses. Furthermore SVM methods also need a huge numbers of the abnormal ISN for training. Finally this made SVM technique not practical as the most of covert communication are not also known. In the given paper we have studied feasible covert channel and then given practical methods for detecting covert channel in the TCP ISN fields that can notice covert channel by using a TCP ISN in the online fashions owing to the mostly reduced computational complexities. Furthermore, simulations result have displayed that the proposed PRMs outperform state of an art method for detecting the covert channel in the TCP ISN in the term of the accuracy and the speed.

REFERENCES

[1] B. Dunbar, A Detailed Look at Steganographic Techniques and Their Use in an Open-Systems Enviroment, SANS (SysAdmin, Audit, Network, Security) Institute, 2002.

[2] M. Owens, A Discussion of Covert Channels and Stegnography SANS (SysAdmin, Audit, Network, Security) Institute, 2002.

[3] K. Szczypiorski, Stegnography in TCP/IP Networks. State of the Art and a Proposal of a New System HICCUPS Institute of Telecommunications Seminar [Online]. Available: http:// www.tele.pw.edu.pl/krzysiek/pdf/steg-seminar-2003.pdf, Retrieved Jun. 2010

[4] R. J. Anderson and F. A. P. Petitcolas, "On the limits of Stegnography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.

[5] S. Attallah, Trusted Computer System Evaluation Criteria, Tech. Rep. DOD 5200. 28-STD, 1985 [Online]. Available: http:// csrc.nist.gov/ publistications/history/dod85.pdf

[6] C. G. Girling, "Covert channels in LAN's," *IEEE Trans. Software Eng.*, vol. SE-13, no. 2, pp. 292–296, Feb. 1987.

[7] M. Wolf, "Covert channels in LAN protocols," *LNCS*, vol. 396, pp. 91–101, 1989.

[8] D. V. Forte, C.Maruti, M. R. Vetturi, and M. Zambelli, "SecSyslog: An approach to secure logging based on covert channels," in *Proc. First Int. Wksp. Systematic Approaches to Digital Forensic Engineering*, Nov. 2005, pp. 248–263. 282 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013

AUTHORS PROFILE

Shaik Rafi, pursuing M.Tech(CSE) from Vikas Group of Institutions (Formerly known as Mother Theresa Educational Society Group of Institutions), Nunna, Vijayawada. Affiliated to JNTU- Kakinada, A.P, India

Boppudi Swanth, working as an Assistant Professor, CSE department at Vikas College of Engineering and Technology, Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India

Betam Suresh, is working as an HOD, Department of Computer science Engineering at Vikas Group of Institutions (Formerly Mother Teresa Educational society Group of Institutions), Nunna, Vijayawada, Affiliated to JNTU-Kakinada, A.P., India