International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 24105-24112

http://www.ripublication.com

Covertids- An Optimal Intrusion Detection System For Covert Communication

N. Vadivelan[1] S.Anbu[2]
Research Scholar, Department of CSE, St.Peter's University,
Professor, Department of CSE, St.Peter's College of Engg.& tech
velancse@gmail.com, anbuss16@gmail.com

Abstract

In real world, cyber-attacks are in rapid development. Various attacks are being attempted to intrude into on-site premises. Various security tools such as firewall, UTM, Gateway security etc. have been implemented over the network & actively monitored, but the real fact was these security tools are compromised to specific attacks within the premises (for eg. backdoors). Covert communication is one among those specific attacks which cannot be detected by the traditional security solution on the premises which are mentioned above. An optimal Intrusion detection system is to be developed to detect covert channels in the active networks. In this paper, an optimal Intrusion detection system has been proposed to detect covert communication attacks. Here the actual model of data's (Host and network) are learnt by the IDS in the network level and in detection phase these learning phase data's are applied and correlated to detect the attack sequence. If the data exhibits the correlation level below than that of the threshold, then the IDS detect the covert channels. Experimental result clearly demonstrates that the proposed IDS can capable to detect the covert communication attacks periodically (Timing channel). The proposed IDS have been modelled using MATLAB R2013b, the simulation results have been pictured into structured graphs.

Keywords: IDS, Covert channel, Covert communication, Network, Anomalies, Host**.**

Introduction

Network is one of the most important technologies used in day to day life. Since there is a vast growth in networking technologies and the growth of threats and attacks in the networking domain is also in increasing number. The best example is the Trojan which alters the entire system of oil bound industries, an advanced terminator STUXNETwhich was reported as the worst ever seen Trojan by the SYMANTEC

Research and development team. A detailed report was available online and has been referenced in the context [3]. Hence according to the context the covert communication in terms of data exfiltration through the compromised host was possible within the premises and possible compromised host can be an insider attack and possible to exfiltrate the small scalable data from the host to the corresponding server. The most common stats was denoted as these possible attacks are always an insider attack and happens within the premises of an organization

The attacks happening inside the organization networks are more hazardous than the attacks happening outside the organization. These types of attacks are basically compromised host of the organization with which was assigned by an extinct code of an employee of the particular organization or through the back door established by the attacker outside the organization. In current state to overcome these attacks various security solutions are provided by the organization for authentication and authorization, yet these attacks are happening over the network.

Some of the security solutions like FIREWALL, IDS & IPS, Anti Hack wall, Watch dog etc. are some the active security parameter of an organization which monitors the data in the average analysis of 24/7/365. Each and every host i.e., every PC's are protected with the high end Anti-virus tool to protect the host against the malware. Since these protections are capable to detect the external behaviour of the network or to analyse the external attacks which are happening outside the organization. Most of the security software's analyse the signature of the current behaviour of each host in the network. Since there are various type of IDS and IPS, these type can be a signature specific, network specific, host specific or anomaly specific, but all of these types can detect only the network intrusion of the known attacks but the outmost specification of covert communication was not alerted or programmed to these security solutions and these software's are not a specific expertized tool to detect the data exfiltration. Hence an optimal IDS to detect the data exfiltration is desirable.

Covert Communication – Problem Statement

In this section the theoretical background of the problem stated was defined and explained. Figures demonstrated in this section denote the real time covert channel establishment and covert communication process. According to the computer security, covert communication is an attack performed to transfer the file illegally from the reliable host with back door to the attacker (server). Traditional security software cannot detect the covert channel attacks because the covert channel utilizes the existing protocol unused header files for establishing covert communications. The covert channels can be easily established in the real time systems which are active in the networks.

Figure 1 and figure 2 denote the sample scenario of the covert communication. Figure 1 denotes the back door installation and covert channel establishment and figure 2 denotes the covert communication between the host and server. Once the host establishes with the attacker (Server) the communication pattern will not be known and it still remains covert. The host and server only know the transmission pattern, two types of active covert channels are timing channels and storage channels, and

here the both channels are in active perspection. Timing channel is established and it is very sensitive in communication and storage channel is insensitive and react according to the protocol based exposure. The main two parameters used for identifying the covert channels are monitoring the protocols at source level or analysing the resource utilization of individual hosts. It is night mare to follow the above mentioned methodologies; hence in this paper we proposed a new methodology to detect the covert communications.

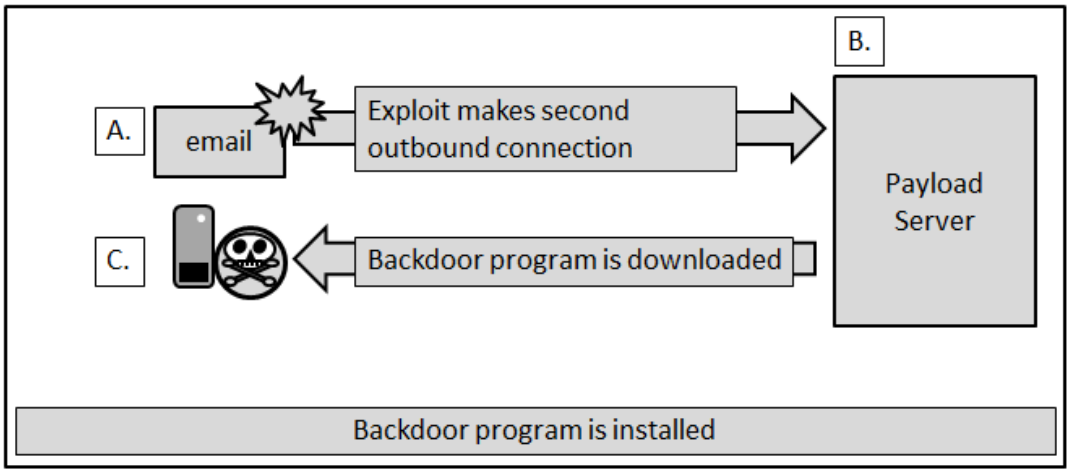

Figure 1: denotes the back door installation and covert channel establishment

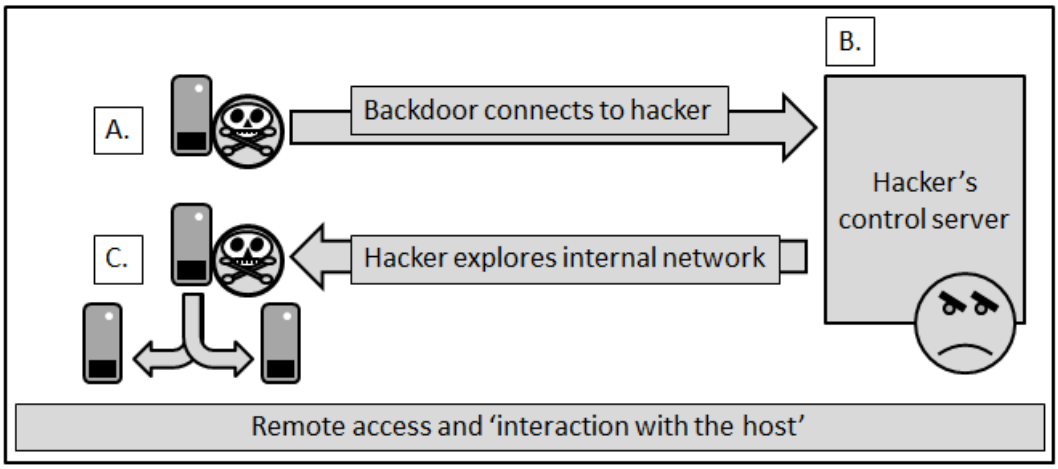

Figure 2: The Covert Communication Between The Host And Server

Here the diagrammatic illustration clearly defines the backdoor installation along with covert channel establishment and possible covert communication in the on-premises network. In figure1 A is the attacker host which sends the backdoor payload URL along with server payload has been sent to the host within the network. B is the

server which holds the payload for the backdoor and C is the compromising host where the back door along with the payload has been installed and compromised, figure 1 clearly defines how the back door has been installed to a host in the network of an organization. Figure 2 explains the working model of the covert communication. Here the payload is initialized in the server and host is invoked, the compromising host acts to the payload server and based on source specification it starts to exfiltrate the data from the compromising host to the server and then to the attacker client.

Proposed Model

The main motto of the work is to detect covert communication in the active networks by analysing the network behaviour. Basically covert communication takes place between the compromised hosts to the server. The data transfer might be within the on premises (possible backdoor). General pattern is analysed for every host in the learning phase at periodical interval. During data transfer if the host which is likely to be compromised is sensitive in sending the vital information at a periodical pattern is analysed and its deviation is monitored from the learning phase. If the deviation ratio is intended to variation beyond the threshold level and the correlated parameters is again analysed to check the covert channels, if the threshold falls beyond the 1 then the pattern is recorded as the covert communication. Data correlation is achieved by comparing the data values with the learning phase and detection phase.

Identifying The Covert Communication?

Covert communication is identified by analysing the basic network parameters along with its resources. The basic system parameters such as CPU utilization, RAM utilization and average network flips along with the jitter is monitors. If the CPU utilization utilizes the high span of clock cycle then there is a timing channel available and when the RAM utilization along with jitter is high in the network flow then there is a storage channel. In generally these parameters were taken into consideration during data transmission. Generally web servers/ local servers do not transfer huge amount of data externally. The basic profiling is achieved by means of SNMP parameters where the protocol stack is monitored. Every packet flow is analysed through WIRESHARK, the network interface level packet analyser.

In this section, two algorithmic views are represented, Computation phase and Detection phase. In computation phase all the input data is learned and in detection phase all the input data and attacking data is correlatedand evaluated.

Computation phase

For all the host in the network
Initialize profiling parameters
Collect network parameters
Do feature selection
Generate pattern for each host
End

Detection phase

For all the host in the network
Initialize profiling parameters
Collect network parameters
Initialize the feature data
Fetch the current data
Generate feature
Compare the feature parameter
Correlate the feature value
If the value is below the threshold of <0.75
Alert "data exfiltration"
Trigger "alarm"
End

Implementation Results

Initially all the network parameters were analysed and features are selected in the learning phase, then the live data is fetched to the detection phase, here the live data is featured and then features are correlated. Figure 3 denotes the storage channel identification by our proposed methodology and figure 4 denotes the timing channel identification by our proposed methodology. We (put have here) collected all the data parameters and analysed both the host learnt data along with the attacking data is simulated in MATLAB R2013b. Our parametric analysis is considered for all the network parameters which were clearly discussed in the above sections.

Table 1: Correlation value beyond the threshold values at each instance

S.No	Time	CPU utilization	Ram utilization	Data flow in bytes
1	4.28	0.0001253	0.001560	0.2223456
2	4.38	0.0002140	0.002456	0.5455646
3	4.45	0.0002345	0.002564	0.6645465
4	4.46	0.0003152	0.002655	0.7866595
5	5.46	0.0010152	0.035650	0.4546469
6	10.15	0.0102560	0.056556	0.6161681
7	10.15	0.0102600	0.056559	0.5183165

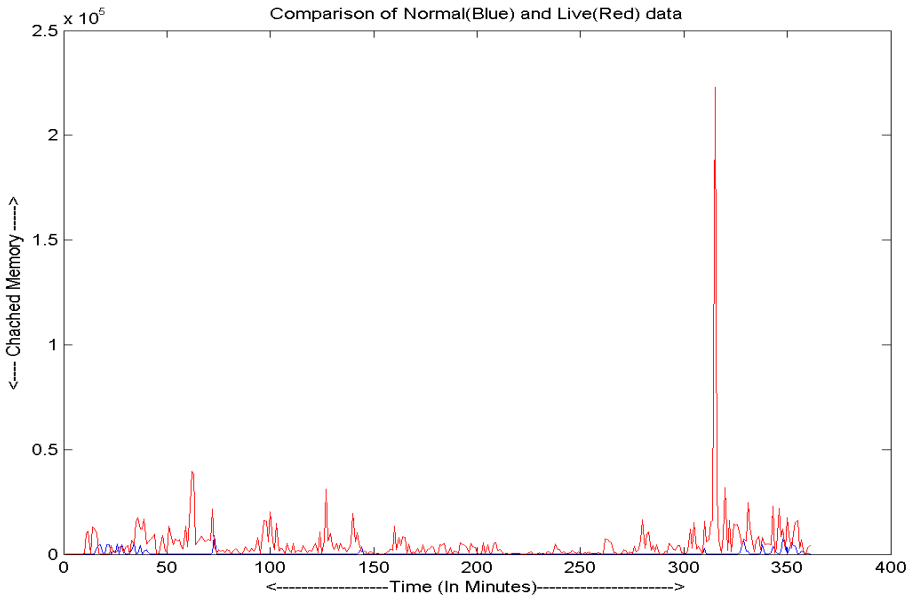

Figure 3: Detection phase – identified storage channel (covert communication)

Figure 4: Detection phase – identified timing channel (covert communication)

Conclusion

Hence we conclude this paper by proposing an optimal methodology to develop an IDS. Figure 4 states the clear illustration of data exfiltration and figure 5 clearly denotes the identification of data exfiltration in covert channels. The key idea of the proposed model is correlating the learning phase along with the detection phase. Here we used the basic network parameters for analysing the data exfiltration possible in terms of timing channels as discussed above. In detection phase,the correlation value compares the possible storage channel and its deviation ration from the learning phase. We have mentioned the worked model along with analysis results which shows the outperforming stats of the proposed model. The proposed model outperforms with better accuracy in identifying the data exfiltration by means of covert communication and works fine for HTTP protocol. In future we would like to enhance our working model for identifying the covert storage channel in context with protocol utilizationfor the specific TCP/IP protocols.

References

[1] Yali Liu "SIDD: A Framework for detecting Sensitive Data Exfiltration by an Insider Attack".

[2] YI Hu "Profiling File Repository Access Patterns for Identifying Data Exfiltration Activities" IEEE 978-1-4244-906-9, 2011.

[3] Data Exfiltration: How data goes out, http://www.csoonline.com/article/570813/data-exfiltration-how-data-gets-out.

[4] Tyrell William Fawcett, Exfild: a tool for the detection of data exfiltration using entropy and encryption characteristics of network traffic.

[5] Amin Hassanzadeh," Intrusion Detection with Data Correlation Relation Graph", The Third International Conference on Availability, Reliability and Security, 0-7695-3102-4/08 IEEE DOI 10.1109/ARES.2008.119,2008.

[6] K.Born, "Browser based covert data exfiltration "in proceedings of the 9th annual security conference, Las vegas,Nevada,2010.

[7] PRTG Network Monitoring http://www.paessler.com/prtg/

[8] Nitha Rachel Suresh, "Security Concerns for cloud computing in Aircraft data networks", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates, IEEE 978-1-908320-00-1/11,Dec 11-14,2011.

[9] Nitha Rachel Suresh, "A Quantitative approach to Browser Exploitation", International Conference on Emerging Technological Trends in Advanced Engineering Research [ICETT2012],ISBN:978-93-80624-624,http://www.icett.com/, February 20-21, 2012.

[10] Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in WSNA '02: Proceedings of the 1st ACM intl workshop on Wireless sensor networks and applications. New York, NY, USA: ACM, 2002, pp. 88-97.

[11] Baggio, "Wireless sensor networks in precision agriculture," in ACM Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Stockholm, Sweden, 2005.

[12] D. Li, K. Wong, Y. Hu, and A. Sayeed, "Detection, classification and tracking of targets in distributed sensor networks," IEEE Signal Processing Magazine, vol. 19, no. 2, pp. 17-29, 2002.

[13] J. Smith and J. Abel, "Closed-form least-squares source location estimation from range-difference measurements," IEEE Transactions on Acoustics, Speech and Signal Processing, vol. 35, no. 12, pp. 1661-1669, 1987.

[14] T. Ajdler, I. Kozintsev, R. Lienhart, and M. Vetterli, "Acoustic source localization in distributed sensor networks," Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on, vol. 2, pp. 1328-1332 Vol.2, Nov. 2004.

[15] Beck, P. Stoica, and J. Li, "Exact and approximate solutions of source localization problems," IEEE TRANSACTIONS ON SIGNAL PROCESSING, vol. 56, no. 5, pp. 1770-1778, 2008.

[16] Bishop, B. Fidan, B. Anderson, K. Dogancay, and P. Pathirana, "Optimal range-difference-based localization considering geometrical constraints," Oceanic Engineering, IEEE Journal of, vol. 33, no. 3, pp. 289-301, July 2008.

[17] N. Bishop, B. Fidan, B. D. O. Anderson, P. N. Pathirana, and K. Dogancay, "Optimality analysis of sensor-target geometries in passive localization: Part 2 - time-of-arrival based localization," Proceedings of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, pp. 13-18, Dec. 2007.