International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 2 [ISSN : 2250-3757]
Publication Date : 30 October, 2015

Exploration of covert schemes and their embodiments in Hybrid Covert channel

-Deep Insight into Covert Channel

AnjanK, Srinath N K, Jibi Abraham and Vinay V Hegde

Abstract—**Covert channels is a vital setup in the analyzing the strength of security in a network. Covert Channel is illegitimate channeling over the secured channel and establishes a malicious conversation. The trapdoor set in such channels proliferates making covert channel sophisticated to detect their presence in network firewall. This is due to the intricate covert schemes that enable to build robust covert channel over the network. From an attacker's perspective this will ameliorate by placingmultiple such trapdoors in different protocols in the rudimentary protocol stack. This leads to a unique scenario of "Hybrid Covert Channel", where different covert channel trapdoors exist at the same instance of time in same layer of protocol stack. For detection agents to detect suchevent is complicated due to lack of knowledge over the different covert schemes. Exploring all the clandestine schemes used in formation of Hybrid Covert Channel would assist in understanding the complete search space of the covert possibilities and thereby improving the knowledgeof detection engine. This can be explored by different schemes available and their entropy impact on hybrid covert channel. The paper sets itself an objective to understand the different covert schemes and their usage in different trapdoors.**

Keywords—Covert Channel, Subliminal Channel, Network Forensics, Kleptography, Trapdoors, Covert Schemes

I. Introduction

With the advent of Internet Of Things (IoT) and its applications there comes an inherent threat of exposure of confidential data over secured channel. Such scenarios are implemented using "Covert Channel"' which compromises very important attribute **"Privacy"**. Covert channel is defined in different ways based on scenarios of covert channel and is non-concrete. Different authors around the globe have defined the covert channel in different ways as the definition is non-concrete and is based on various scenarios of the covert channel.

"A covert channel is a malicious and hidden communication by two or more entities in a legitimate network communication".

Covert Channels clearly violates the security policies laid down by the network environment allowing the information leak to the unauthorized receiver.Covert Channels can be implemented at any level that is at thread level, Operating System level, between resources, in communication networks and in virtualized environments like SAN and Cloud. A simple covert channel can be visualized in the figure 1 where channel comprises of both covert and overt channel in the communication.

Fig. 1. Covert Channel Visualization

Covert channel information exchange is based covert languages pre-negotiated by the covert users and implementation of such languages uses intricate encoding schemes. These schemes may be proliferated into multiple protocols, where each such protocol will be a trapdoor. This makes it complex to detect such clandestine mediums. SETUP [18] attacks makes uses of multi-trapdoor mechanism for ameliorated development of covert channel. A hybrid covert channel scenario may have such multiple trapdoors either in the same layer on in different layers.

Multiple trapdoors can be implemented in the same layer or in different layers .Implementation of the different covert channel variants at the same instance of time tends to behave as a single coherent covert channel. This channel is termed as "Hybrid Covert Channel". A Hybrid Covert Channel [3] is a variant of covert channel that is homogeneous composition of two or more covert channel variants existing at same or different instance of time. Hybrid covert channel may not have strict composition. It becomes complicated to assess the composition of the Hybrid Covert Channel. An instance of the hybrid covert channel is depicted in the figure 2 and the composition can be a simple network covert channel in the TCP and subliminal channel in the TLS; both being a transport layer protocol.

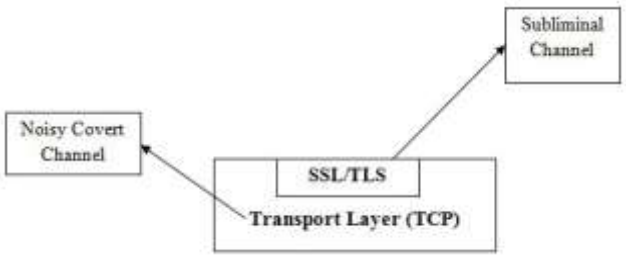

Fig. 2. Hybrid Covert Channel in Transport Layer

The covert channel was first introduced in the traditional confinement problem as described in [11]. Ever since the discovery of covert channel there has been an extensive

work carried out on devise detection methods, which detect only covert channel either on live wire or by forensics methods [6]. Detections are also based the covert channel variant [3][7] and the scenario set in the environment.

Covert channel detection [14] is based on detecting covert shells by monitoring the unusual traffic in the network stream. Covert timing channels are designed and detected [13] based on packet inter-arrival and modeling whole process as Poisson's distribution. Illegal information flows in covert channels are tracked by tracing the Message Sequence Charts (MSC) [9]. This paper employs a statistical protocol based detection [1] to detect hybrid covert channel based on analysis made on packet headers.

Further section of this paper covers variants covert schemes and their usage in different scenarios. Section 2 explores covert communication types. Section 3 explores the covert encoding scheme and its embodiment in protocols. Section 4 discuss about metric and measurement of covert schemes. Conclusion and future works is provided in section 5.

II. Covert Communication Types

In Network communication, covert communication amongst a pair of users can take two forms;

- covert data exchange and
- covert indication

In covert data exchange, covert data is exchanged between the covert users by hiding covert data in rudimentary protocols. This form of covert communication can best be understood with pipeline problem, where there exists two pipes p_1 and p_2 of diameters d_1 and d_2 respectively, one inside the other such that $d_2 < d_1$. These pipes are setup between two geographical places for the transportation of crude oil. In Figure 2, the inner pipe p_2 of diameter d_2 is the covert pipe not known or undocumented in the design and used for smuggling oil. The outer pipe p_1 is the legitimate pipe. This type of the covert communication type will not have pre-defined encoding schemes will be simple placement of covert data (trapdoor creation) directly in to the identified clandestine field in the traditional network protocol stack. This channel is called as simple network covert channel.

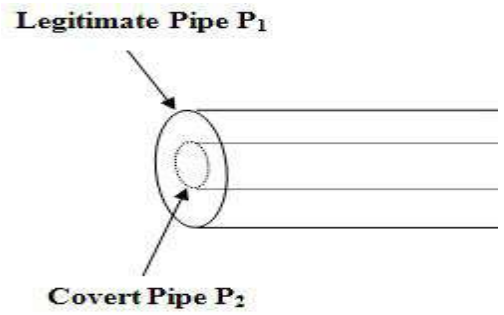

Fig.2 : Classical Pipeline Problem

Second form of covert communication is the covert indication. Covert users communicate in a language not known to others. In Figure 3, the covert sender and receiver share an information encoding scheme to leak information. This information encoding scheme as seen from the figure 1 is the language that covert users employ to communicate in a secured legitimate network environment. This sophisticated communication is visible to our detection engine, however decoding the language might be quite difficult in many situations.

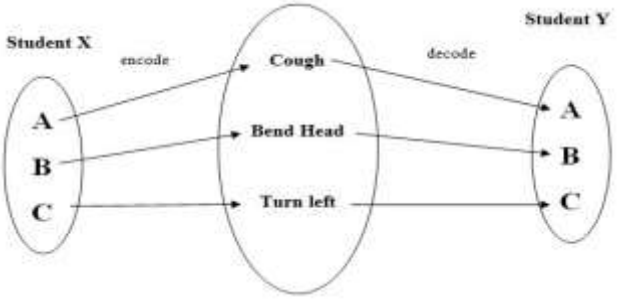

Fig.3: Classical Examination Problem

The best real time classical example of such communication is Examination Problem. Student X leaks the answers to Student Y for an objective type examination paper in an examination hall in presence of invigilating officer. For each choice in a question, student X makes a gesture that triggers an event to student Y. For instance to communicate choice A to student Y, student X coughs. Same holds well in case network communication where covert user X triggers continuous clock events that communicate some form of action to be performed by covert user Y.

Some of the other forms of covert indication in network scenario include-

- Encoding ASCII character set in Sequence number. Decoding the same by applying mathematical operation on sequence number. This can either be in TCP or In IP ID fields.
- Repeated sending of acknowledge packet to an unknown server where the covert receiver is listening to. Receiver has to count the number of time the acknowledge packet was sent to this server. This value can later on mapped to ASCII table for retrieving suitable character.
- Retrieving the packet sorting order numbering in IPSec frames which serves as information to the covert receiver.
- Using logical operators like the XOR with sequence number to get the covert data.
- able to reliably detect whether communication is happening.

III. Covert Schemes and their embodiment

The covert schemes are crucial for conveying the covert data over communication channel in a obscured way. More sophisticated scheme likely not to be retrieved by detection

entity. Few samples of covert schemes were discussed in section 2 of this paper and detailed schemes are presented here.

Scheme 1

The IP ID is field used for identification of the packet and is used for the routing purpose. The covert scheme used for this field is based on following strategy-

- Intentional use of only certain IP ID's while having conversation with Covert receiver.
- Scheme is designed by the covert sender for embedding covert characters in to the IP ID field.
- The Covert receiver applies the scheme used by the sender to retrieve the covert character.

For instance a simple scheme that can be used is by extracting the value in IP ID and performing modulus operation with the size of the character set. General notation for this scheme for encoding a character 'c' is

$$E(c) = (R-1) mod\ n$$

Where $E(c)$ is the encoding function, R is the IP ID value and n is the size of the character set.For an ASCII character set, $n = 256$

Example: If IP ID = 26702 and if the character to be sent is `M' then E(M) = 26702-1 mod 256 = `M'.

To convey a covert message, the covert sender has to select IP ID in such a way as to match with $E(c)$.

Scheme 2

Another prominent scheme used is on the sequence number where maximum range is 4,294,967,296 numbers as it is 32 bit field. To communicate covertly under this scheme following strategy is employed-

- Sequence number is multiplied with value of character set and bound is declared with maximum limit.

- The receiver side retrieves the sequence number and then divides it by character set size.

The encoding function $E(c)$ is given below-

$$E(c) = (S * n)$$

Where S is the initial sequence number and n is the size of the character set. The decoding function is $D(c')$ is given below -

$$D(c') = S' / n$$

Where c' is the decoded character and S' is the received sequence number.

For instance to send an character `I' covertly over the channel, the sender would have to choose 1235037038 as sequence number and the maximum value is derived as $65535 * 256 = 16777216$

Therefore the decoded character is $D(c') = 1235037038/16777216 = 73$, The value 73 when mapped back to ASCII Table is the character 'I'.

Scheme 3

Another scheme which has tremendous effect on the bandwidth is the modulation of TCP timestamps or use of timing element in the network protocol. TCP timestamps is in the options field of the TCP header which indicates the round trip time of the packets. The TCP process accurately calculates the next retransmission of TCP segment which was failed to be acknowledged. If the character is to be covertly sent using this scheme following strategy is used.

- Get the binary representation of the character and extract bits from the least significant bit.
- Check if the Timestamp least significant bit(LSB) is same as covert bit,if so send the TCP segment.
- Covert receiver will extract the LSB of the timestamp and store the same until it is a byte.

Let B_c be the binary representation of the character 'c' and $F_{LSB}(B_c)$ be the encoding function for encoding the covert bits in TCP timestamp.

IV. Entropy based covert channel analysis

The entropy [2] in communication network indicates the number of bits required to encode a character over the channel as stated by Shannon Entropy theory. This is based on the frequency of the characters in given string and the size of the alphabet. The entropy measure also checks for uncertainty of the random variable.

Let A be finite set of characters such that $|S| \geq 1$and any character '$c' \in A$. A sequence of symbols which is a string, each of alphabet in string ∈ A. For instance let character string ``cbbacabbac'' be sequence of symbols that needs to be transmitted over network; then its sequence of corresponding bits represents the coded symbol sequence which may be ``01100011 01100010 01100010 01100001 01100011 01100001 01100010 01100010 01100001 01100011'' . Then the entropy for such scenario is defined as –

$$H(p_i) = \sum_{i=1}^{n} p_i \log_2 p_i$$

where$i \in |S|$ and $|S| \geq 1$, p_i is the probability of the occurrence of symbol c in the string and n gives the length of the string.To transmit a message ``network''

over the communication network, following are the calculated entropy for each alphabet –

The frequency of all the characters in a string with unique symbols will be same, since the word ``network'' has unique symbols the frequency is 0.143. Let X be string for which the entropy is to be calculated, here X may word like network or stream of numbers then

H(X) = [(0.143 log2 0.143) + (0.143 log2 0.143) + (0.143 log2 0.143) +(0.143 log2 0.143) + (0.143 log2 0.143) + (0.143 log2 0.143) + (0.143 log2 0.143)]

$$H(X) = 2.803$$

It requires 3 bits to represent each symbol in the given string and 21 bits are required to represent the entire string. Further the appropriate line coding technique has to be chosen to represent them in the transmission line. So in general entropy of X where each alphabet is a unique symbol is

$$H(X) = 3\ x\ |X|$$

In a covert channel scenario, the covert user has to be chosen the message in such a way that the entropy of string should always be less that number of bits available for that field in the protocol header.

$$H(X) < |Maximum\ number\ of\ bits\ in\ that\ field\ (B_f)|$$

The IP ID presented in the scheme 1 of this paper has 16 bits in the IP header, so to send X the minimum of 21 bits are required. hence capacity of the covert channel is

$$C_C = \log_2 \frac{16}{21} = 0.25$$

The covert channel occupies 25% of total IP header space. Multiple trapdoors (t) [6][7]in IP header or protocol header simply doubles the covert channel capacity. However the entropy to channel capacity ratio will be low thus making it robust i.e.,

$$\frac{0.25x2}{2.803} = 0.17$$

This makes the detection of covert bits much difficult as the detection systems needs to scan more fields for analysis.

In general,

$$\frac{C_C * t}{H(X)} < H(X)$$

for robust covert channel construction where η [8]the covertness index for such multi-trapdoor covert channel will be greater than 0.5. The multiple trapdoors through a protocol or set of protocols is actually setting up of multiple covert channels in the communication network. The entropy for such scenarios is dispersed across multiple making it difficult to understand the scheme. The scenario of multi-trapdoor covert channel behaves like single coherent hybrid covert channel where the effect of the entropy is doubled. The below results shown in the figure 4 and figure 5 shows the accurate expected behavior discussed in this paper –

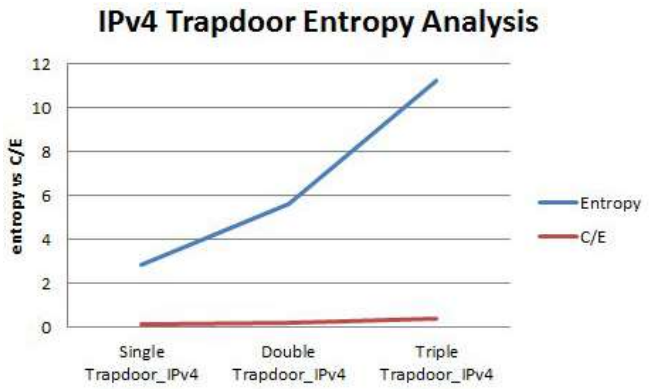

Fig.4 IP Entropy analysis

The results indicate the multiple trapdoors used in hybrid covert channelyields to a higher entropy value and low channel to entropy ratio (C/E). Theconstant C/E ratio also indicates the consistent usage of protocol header forconstructing multi-trapdoor based hybrid covert channel. This implies that thecovert schemes used in Hybrid covert channel is difficult detect in secured communication.

Author Affiliation

Anjan K, Assistant Professor, Dept. of Computer Science and Engineering, R V College of Engineering, Bengaluru, India.

Dr. N K Srinath, Professor and Dean Student Affairs, Dept. of Computer Science and Engineering, R V College of Engineering, Bengaluru, India.

Dr. Jibi Abraham, Professor and Head, Dept. of Computer Engineering and Information Technology (CEIT), College of Engineering Pune, India.

Prof. Vinay V Hegde, Associate Professor, Dept. of Computer Science and Engineering, R V College of Engineering, Bengaluru, India.

Conclusion

Covert schemes are difficult to understand from third party entity as they obscure the content taken in protocol header. This provides an opportunity for embedding any data which may even be malware code. Entropy based analysis gives the actual number of bits used to represent the covert symbol in a protocol. This gives clearly metric to understand the covert channel schemes in a better way. It is unacceptable to have malicious conversation of the network even in presence of administrator. It is inference this experiment that the hybrid covert channel has high degree of entropy which makes it difficult to detect. It isrequired to concentrate on stronger detection principle to detect such events**.**

Acknowledgment

Prof. Anjan K would like to thank Late. Dr.V.K Ananthashyana, former Head, Dept. of CSE, MSRIT, India

for igniting the passion for research. His vision and aspiration has inspired me to pursue and reach completion of my Ph.D research work.

References

[1] Description of Detection Approaches at the URL. http://gray-world.net/projects/papers/html/cctde.html, 2014.[Online; accessed 15-Feb-2015]
[2] Description of the Entropy calculation at the URL. http://www.shannonentropy.netmark.pl/, 2014. [Online; accessed 16-Feb-2015].
[3] Koundinya Anjan and Jibi Abraham. Behaviour analysis of transport layer based hybrid covert channel. In Third International Conference on Network Security and Application, pages 83-92, Chennai, India, 2010. Springer-Verlag LNCS series.
[4] Jibi Abraham Anjan K, Srinath N K. Attack modeling and behavioralanalysis of hybrid covert channel in secured communication. ACEEE International Journal of Network Security, 05(2):67-77, 2014.
[5] Bo Yuan Chaim Sanders, Jacob Valletta. Employing Entropy in the Detection and Monitoring of Network Covert Channels. 2012.
[6] Rajarathnam Chandramouli and Koduvayur P. Subbalakshmi. Covert channel forensics on the internet: Issues, approaches, and experiences. 5(1):41-50,July 2007.
[7] Anjan K Koundinya et.al. Covertness analysis of subliminal channels in legitimate communication. In ADCONS 2011, pages 582-591. Springer-Verlag LNCS series, 2012.
[8] Jaideep Chandrashekar et.al. Exploiting temporal persistence to detectcovert botnet channels,. In Proceedings of 12th International Symposium,RAID 2009, pages 326{345, Saint-Malo, France, September 2009
[9] Lo□_c H_elou□et, Claude Jard, and Marc Zeitoun. Covert channels detection in protocols using scenarios. SPV'03, Volume 3, April 2003.
[10] Anjan K Koundinya and Jibi Abraham. Design of Transport Layer BasedHybrid Covert Channel Detection Engine, volume 1 of 4. InternationalJournal of Ad hoc,Sensor and Ubiquitous Computing, 2010.
[11] B. W. Lampson. A Note on the Con_nement Problem. Communication ofthe ACM, 1973
[12] Enping Li and Scott Craver. A supraliminal channel in a wireless phone application,. In Proceedings of the 11th ACM workshop on Multimedia and security, pages 7-18, Princeton, New Jersey, USA, 2009.
[13] Clay Sheilds Sarder Cabuk, Carla Brodley. IP covert timing channels : Design and detection. CCS, 4, 2004.
[14] Clay Sheilds Sarder Cabuk, Carla Brodley. Ip covert channel detection. ACM Transaction on Information and System Security, Volume 12(Article 22), 2009.
[15] Gustavus J Simmons. The Subliminal Channel and Digital Signatures. Springer-Verlag, 1998.
[16] Steffen Wendzel. Protocol Channels. HAKIN9, 2009
[17] Andreas Willig. A short introduction to queuing theory. lecture notes at Technical University, Berlin, 1999.
[18] Adam Young and Malicious Cryptography. First edition. Wiley Publishing,Feb, pages 220-240, 2004.

About Author (s):

Anjan K has received his B.E degree from Visveswariah Technological University, Belgavi, India in 2007 And his master degree from Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore, India. He has been awarded Best Performer PG 2010 for his academic excellence. He is pursuing Ph.D in Computer Science and Engineeing from VTU, Belgavi. He is currently working as Assistant Professor in Dept. of Computer Science and Engineering, R V College of Engineering, Bengaluru, India.

Srinath N K has his M.E degree in Systems Engineering and Operations Research from Roorkee University, in 1986 and PhD degree from AvinashLingum University, India in 2009. His areas of research interests include Operations Research, Parallel and Distributed Computing, DBMS, Microprocessor. His is working as Professor and Dean Studetn Affairs, Dept of Computer Science and Engineering, R V College of Engineering.

Jibi Abraham has received her M.S degree in Software Systems from BITS, Rajasthan, India in 1999 and PhD degree from VisveswariahTechnologicalUniversity, Belgavi, India in 2008 in the area of Network Security. Her areas of research interests include Network routing algorithms, Cryptography, Network Security of Wireless Sensor Networks and Algorithms Design.She is working as Professor and Head in Dept. of CEIT, College of Engineering Pune.

Prof. Vinay V Hegde has received his B.E degree from Visveswariah Technological University, Belgaum, India in 2004 And his master degree from Department of Computer Science and Engineering, R V College of Engineering, Bangalore, India. He has submitted his research work to Avinashilingam University, Coimbatore. His areas of research include Natural language. He is currently working as Associate Professor in Dept. of Computer Science and Engineering, R V College of Engineering.