Towards a Reliable Detection of Covert Timing Channels over Real-Time Network Traffic

ABSTRACT

- Inter-packet delays (IPD) of legitimate network traffic can be exploited for information hiding purposes and distribution of secret and sensitive data. This process is known as Covert Communication and poses a grave threat to networks and other Internet. In this paper we propose a novel approach to detect Covert Timing Channels (CTC) activities based on IPD distributions of network traffic. We present and leverage three different non-parametric statistical tests that can be used to generate very different statistical test scores for overt and covert traffic IPDs.
- Our new detection approach is designed around two major benefits: Firstly, the new detection approach can detect various CTC algorithms that have similar impact on network traffic IPD distributions. Secondly, our detection approach reliably detects covert communication over online network traffic with minimal lag between start of covert activity and the point of detection.

Cont…

- We have evaluated and verified the reliability and effectiveness of our detection approach utilizing a large number of overt and covert traffic streams and various scenarios of the proposed detection technique.
- The obtained results show that the new detection approach can precisely differentiate between overt and covert network traffic and detect covert communication activities over 90% of time on average.

EXISTING SYSTEM

- This information hiding approach is known as covert communication. The presence of this hidden information, or covert data, is only known to the covert sender and covert receiver, which are equally aware of the employed covert channel algorithm.
- Depending on the type of properties used for conveying covert data, covert channels are generally categorized as Covert Timing Channels (CTC), Covert Storage Channels (CSC), Covert Hybrid Channels (CHC) and Covert Behavioral Channel (CBC). CTCs take advantage of packet inter-arrival times to encode covert data by modulating the packet gaps, while the CSC approach inserts data into packet fields of a given communication protocol.

PROPOSED SYSTEM

- In general, our detection technique uses non-parametric statistical tests that compare two sample observations based on their values and distribution.
- Sample observations are covert and overt network traffic IPDs that are collected from implementing the case study CTC algorithms over a real network environment, as well as generating different overt traffic flows based on various distributions and parameters.

Hardware requirements

Processor	-	Pentium-IV
Speed	-	1.1 Ghz
RAM	-	256MB(min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

SOFTWARE REQUIREMENTS

Tool	-	Network Simulator-2
Operating system	-	LINUX
Front end	-	OTCL (Object Oriented Tool Command Language)

REFERENCES

[1]. H. Zhao, Y. Q. Shi. “A phase-space reconstruction approach to detect covert channels in TCP/IP protocols”. In Information Forensics and Security (WIFS), IEEE International Workshop on (pp. 1-6). December 2010.

[2]. G. Garateguy, G. R. Arce, J. Pelaez. “Covert channel detection in VoIP streams”. In Information Sciences and Systems (CISS), 45th Annual Conference on (pp. 1-6). March 2011.

[3]. S. Cabuk, C. E. Brodley, C. Shields. “IP covert timing channels: design and detection”. In Proceedings of the 11th ACM Conference on Computer and Communications Security (pp. 178-187). October 2004.