Entropy based approach to detect covert timing channels

By Xiuwei Yi, Dhaval Patel

Introduction

The paper focuses on a new approach to detect covert timing channels that is based on a new entropy approach. A covert timing channel alters the timing of network events to secretly transfer packets of data. The data is transferred via the Internet. The process of detection of such channels is still a challenge to this day, and innovators continue to search for an easy alternative. So far, developers have managed to create detection methods that target a specific channel. However, there can be more than one channel. As of the present, there is exists no method that can be used to handle all the channels at once. Entropy has never been used to detect covert timing channels. Entropy connotes the measure of uncertainty or information content (Gianvecchio & Wang, 2006). One cannot determine the exact entropy rate. However, corrected conditional entropy is designed to be accurate (Gianvecchio & Wang, 2006). In addition, one can get accurate results using limited data which makes it easier to conduct a study.

The aim of the first phase of the study is to determine whether this new approach can differentiate between covert and legitimate traffic. The technique adopted was the fine-binned estimation of entropy and the coarse binned estimation. The results derived showed that the use of entropy and corrected conditioned entropy can identify covert timing channels (Gianvecchio & Wang, 2006).

Background and Related Work

The disruption of covert timing channels negatively affects the traffic. Even though it reduces the capacity of covert timing channels, it decreases system capacity. Covert timing channels can be detected using statistical tests. Earlier efforts in the area were on disrupting covert timing channels or on eliminating the same in the design systems.

Covert timing channels are either active or passive. Active channels generate traffic while stealing data. Passive ones, on the contrary, manipulate the timing of existing traffic (Gianvecchio & Wang, 2006). Majority of the covert timing channels that were studied for purposes of this research paper were active. According to Gianvecchio & Wang, the types of timing channels that have been focused on before include the following (2006):

- IP covert timing channel
- Time-replay covert timing channel
- Model-based covert timing channel
- Jitterbug
- A binary covert timing channel
- Cloak

Detection tests are either classified as shape or regularity tests. Shape tests focus on first order statistics to determine the shape of traffic. Regularity tests use second or higher order statistics to detect covert timing channels. Another detection test that can be used is the Є-similarity test. It is designed to detect IPCTC and Cloak covert timing channels.

Entropy Measures

The entropy rate is the conditional entropy of a sequence of infinite length (Gianvecchio & Wang, 2006). In this section, we look at the different entropy measures available with special focus on corrected conditional therapy. Highly complex processes tend to have a high entropy rate. A regular process, however, has a low entropy rate. The entropy rate can be at zero for rigid periodic processes as they have a repetitive pattern.

Corrected Conditional Entropy

It has already determined that an entropy rate can only be estimated. This process entails the replacing of probability density functions with empirical probability density functions (Gianvecchio & Wang, 2006). This is done using the histograms method. The definition of the corrected conditional entropy is determined using the percentage of unique patterns of length and a fixed entropy rate of 1. The corrective entropy decreases while the corrective term increases.

The next step is to implement binning strategies. This is critical for the test to be effective. According to Gianvecchio & Wang, the importance of this one can be determined by examining the following:

1. The method of data partitioning
2. The bin granularity

Past studies show that equiprobable bins produce better results since it makes it easier to determine the bin number for a value based on the cumulative distribution function.

Since the main objective is to effectively detect covert timing channels with minimal disruption to system operations, it is necessary to determine the rate of efficiency of tests. This is necessary especially where the tests are run on real-time.

The Effectiveness of the New Approach

This section covers the experimental approach used. The new system of detection can only be validated through experiments. The tests were conducted against four covert timing channels: IPCTC, TRCTC, MBCTC, and Jitterbug (Gianvecchio & Wang, 2006). The entropy test is then compared to two other detection tests: Kolmogorov-Smirnov test and the regularity test (Gianvecchio & Wang, 2006).

How effective a test is depends on false positive and true positive rates. The preferred result is a low false positive rate and a high true positive rate (Gianvecchio & Wang, 2006). How effective a detection test is depends largely on the mean, variance, and distribution of test scores. The Kolmogorov-Smirnov test uses the training sets of legitimate traffic to determine the behavior of legitimate traffic (Gianvecchio & Wang, 2006). The test measures the distance between the training set and the test sample to determine legitimate behavior. The test focuses on the shape of the traffic similar to the entropy and corrected conditional entropy.

The test was run 100 times for 200 packet samples of legitimate traffic (Gianvecchio & Wang, 2006). The test results based on the four covert traffic channels that were used in the tests conducted will be discussed in the subsequent sections.

IPCTC

This is the simplest covert timing channel and the simplest to detect owing to its abnormal shape and irregularity (Gianvecchio & Wang, 2006). The scores registered a lower score for IPCTC than for legitimate traffic. The regularity test fails in this case as it measures sets of 100 packets rather than the legitimate traffic. This makes it impossible to differentiate between IPCTC and legitimate traffic. As such, it is necessary to examine more than the average test score (Gianvecchio & Wang, 2006).

TRCTC

This covert timing channel is more advanced since its shape is similar to that of legitimate traffic. However, the irregularity I found concerns how similar the shape appears. It is too perfect. The test scores for the Kolmogorov-Smirnov and entropy tests show both legitimate and TRCTC traffic to be almost the same. Since the tests only measure first-order statistics, they are unable to detect the irregular traffic. The corrected conditional entropy test gives a similar result to that of IPCTC where the mean score for both TRCTC and legitimate traffic are very close in range. Since the test has detection rate of 1.0, it is the only one that makes it easy to detect TRCTC traffic.

MBCTC

This covert timing channel is more advanced as it mimics legitimate traffic. The Kolmogorov-Smirnov test registered high MBCTC scores compared to those of legitimate traffic. However, this was less than the standard deviation. The entropy test scores have a higher MBCTC average compared to that of legitimate traffic. This shows the great similarity between the two. In contrast, the corrected conditional entropy scores reveal lower MBCTC scores than that of legitimate traffic. This makes the test the most effective as it has a 0.95 detection rate (Gianvecchio & Wang, 2006).

Jitterbug

This is a passive covert timing channel. As such, it manipulates inter-packet delays of legitimate traffic. Other than the corrected conditional entropy test, other tests reveal a very low detection rate of 0.04. This further proves that the corrected conditional entropy test is more accurate.

Conclusion

This paper presents a new tool for detecting covert timing channels. The use of both entropy and corrected conditional entropy provide better detection results than all the other tests used. This is especially crucial since the effectiveness of detection tests is based on their ability to differentiate between legitimate traffic and covert timing channels. Owing to the low variance, the entropy test is sensitive to small irregularities that can be in traffic. However, it would be necessary to conduct tests on other covert timing channels to determine how effective this method of detection is. So far, it has yielded the most promising results compared to other detection tests.

References

Gianvecchio, S., & Wang, H. (2006). *An entropy-based approach to detecting covert timing channel.* Virginia: College of William and Mary.

.