MODELING NETWORK CONVERSATION FLUX FOR PATTERNLESS INTRUSION DETECTION

Stephen D. Donald, Robert V. McMillen, David K. Ford, and John C. McEachen
Re-configurable Intrusion Detection Laboratory Research (RIDLR)
Department of Electrical and Computer Engineering
Naval Postgraduate School
437 Dyer Road, Code EC/Mj
Monterey, California 93943, USA

Abstract – A novel system for conducting non-signature based, or patternless, intrusion detection of computer networks is presented. This system uses principles of thermodynamics to model network conversation characteristics. Observing the properties of entropy, energy and temperature within the system develops a notion of baseline operating conditions. Perturbations in these properties are considered potential intrusions for further investigation. Preliminary results indicate this system has significant potential for revealing anomalies in large network systems.

Key-Words: Patternless network intrusion detection, entropy, statistical mechanics

1 Introduction
By definition, an intrusion is somebody attempting to break into or misuse your system. The word “misuse” is broad, and can reflect something as severe as stealing confidential data to something benign such as misusing network resources. An Intrusion Detection System (IDS) is a system for detecting such intrusions [1].

An IDS’ primary means of identifying an intrusion is by the use of signatures. Signatures are predefined patterns that may indicate a specific attack or anomaly. A signature based IDS monitors network traffic searching for bit patterns that match its database of signatures.

The use of signature patterns to identify intrusions is a quick and efficient process at the expense of flexibility and adaptability [2]. IDS developers constantly produce signature updates because, if a signature is not in the database, the IDS will not detect the intrusion. Also, due to the availability of malicious software on the Internet, anyone with sufficient knowledge in computer programming can make quick modifications and produce undetectable malicious code.

This paper presents a method that will potentially allow a network analyst to use other means (non-signature based) to detect and identify intrusions. The process described in this document does not depend on signatures. Rather, it uses a mathematical model [3] to graphically represent the network’s general characteristics using thermodynamic principles such as energy, entropy, and temperature.

The use of thermodynamics in modeling network-related information has been investigated previously, most recently in the analysis of quality-of-service (QoS) in asynchronous transfer mode (ATM) networks ([4]). This approach differs from the one in this paper in that they measure an artifact (e.g. – bandwidth) of the information exchange as opposed to a characteristic of the exchange itself (i.e. – the communicants). We assert that our method provides a more general abstraction of how the network being used at a given moment in time.

Burgess [5] has presented similar research that models computer networks using the concepts of statistical physics. While his paper provides a hypothetical analysis, he does not provide any applied analysis and makes no consideration for actual implementation.

The intent of this system, dubbed Therminator, is not to replace existing IDS technology but complement it. The combination of the two will hopefully benefit from the routine update of the commercial IDS signature database, which provides speed and efficiency. Ideally then, when Therminator identifies an event not known to the IDS, a new signature can be developed by using the data acquired by the Therminator sensor. Also, the “false-alarm” rate (IDS identifies a friendly event as hostile) can be reduced by correlating the output of the two systems. This correlation will ensure the analyst can distinguish an IDS attack from an actual attack on the network.

2 Thermal Properties Of Network Traffic
As was stated before, the goal of Therminator is to reduce standard network data into a useful,
reproducible, and meaningful form, ultimately to allow accurate detection of network anomalies. To do this, the statistical mechanics process is going to be reversed, entering the process with a notion of continuously observed microscopic state transitions and exiting with macroscopic notions of entropy, energy, temperature, work and heat. The notion of state will be more carefully defined below, but quickly summarizes into activity levels of various conversation groups within the network. The Hamiltonian is, in effect, the aggregate set of rules that govern the conversations, including protocol interactions as dictated by the Internet Engineering Task Force’s (IETF) Request for Comments (RFCs), actual and logical network architecture, and such amorphous entities as security restrictions and usage policies. It is however the state transitions that are observed. One end product is a real time graphical description of the configuration of the network.

A. Buckets & Balls = States

The state model used by Therminator tries to model the typical characteristics of network traffic while providing a usable notion of state for the thermodynamic calculations. At the most basic level, Therminator’s view of network state is a collection of network conversation groups and their respective relative information levels. A state transition will be an exchange of information elements between the involved conversation groups. The analogy used during development describes the conversation groups as buckets and the information element as balls. A bucket will contain some ordinal number of balls, and the collection of buckets and their respective number of balls will be the state of the network. The bucket can be defined using any combination of conversation characteristics including who is talking (individual hosts or networks), the language they are speaking (TCP, UDP, or ICMP), or the job they are performing (client or server). The implemented model can use any field within the sensed data to define conversation groups. A ball is a relativistic representation of the information a bucket contains. A state transition causes a shift in the distribution of information between the buckets. This model translates network behavior into state transitions by selecting a ball from the bucket matching the source characteristics of the packet and moving that ball into the bucket matching the destination characteristics of the packet, thereby redistributing the information and transitioning the state.

For example, bucket A defines the conversation group containing hosts X and Y, while bucket B defines the conversation group containing host Z. Each bucket will be initialized with 3 balls yielding a starting state of {3, 3}. For this example, the starting state is arbitrary, a more detailed analysis of starting state and boundary selections will be discussed below. The following information exchanges are recorded transiting the network: YÆZ, ZÆY, XÆZ, YÆZ, and XÆY. Applying the Therminator state transition model, upon receipt of the first YÆZ exchange a ball is selected from bucket A, which matches the source characteristics of the exchange. That ball is then placed into bucket B, which matches the destination characteristics of the exchange. The result is a transition to a new state of {2, 4}. The next exchange, ZÆY, removes a ball from bucket B and places that ball into bucket A, resulting in a revisit to the state {3, 3}. XÆZ removes a ball from bucket A and places it into bucket B revisiting the {2, 4} state. A YÆZ exchange occurs again resulting in a transition to the new state {1, 5}. Finally, the XÆY exchange repeats the previous state {1, 5}, because the state transition model causes the ball to be removed from bucket A and then placed back into bucket A. In summary, the exchanges YÆZ, ZÆY, XÆZ, YÆZ, and XÆY result in the states {2, 4}, {3, 3}, {2, 4}, {1, 5}, and {1, 5} when given an initial state of {3, 3}.

Figures 1 and 2 show the importance of the state walk, and how the model provides more information than a simpler model. Both graphs represent a state space made up of two conversation groups, bucket A and bucket B, and they start with 5 balls each. As stated before, a network exchange can cause a state transition in three ways: by moving a ball from bucket A to bucket B, by moving a ball from bucket B to bucket A, or by either moving a ball from bucket A to bucket A or bucket B to bucket B, essentially resulting in no change for that period.

The paths shown in the figure 1 and 2 share a few notable similarities. The paths begin and end at the same state and undergo the same number and types of state changes, including five changes up, seven down, and four no changes. However, the transitions that make up those changes produce remarkably different paths, shown on the left hand side of the figures, and those paths produce remarkably different state counts, shown on the right hand side of the figures. Thus it is shown that this model provides a number of unique discriminators including number and type of state changes, starting and ending point and the general path in-between, and the state counts. Because of these discriminators, this model produces information that
can be used to assist processing and visualization of the network. Specifically, it can be shown that the graphs on the right hand side of Figures 1 and 2 are essentially probability distributions of the state, and that the distribution is analogous to the classic thermodynamic Boltzmann curves [6]. This information offers a unique visualization technique of network activity.

It should be noted that the examples used in this section were chosen to easily illustrate the concepts of state, state space, and state walk. The examples do not clearly depict the ability for examining anomalous behavior, which comes from using a higher dimensional bucket space. In fact thermodynamics was developed just for the purpose of data reducing such very high dimensional paths. Anything beyond two dimensions is difficult to illustrate on paper, especially when trying to show how those dimensional values change over time. One of the best ways to examine the capability of detecting anomalies is to think of the state’s walks occurring in multiple planes. If the state space can be well defined then all the normal activity might well occur on a single plane. When an anomalous event occurs, the state transition causes the state walk to shift to a higher plane. The anomalous state walk continues to follow a similar path as the normal state walk, however, the path is on a different plane, generating a series of different states, and resulting in a remarkable different energy, entropy, temperature, and probability curve.

A. States & State Counting = Probability

Once the states are defined, the next step in the Therminator process is to determine the individual probability of each state. Each state will have a total time in which the network occupied that state and the number of times that the state occurred. The probability, $P$, for a given state simply equals the time, $k$, dedicated to that state over the sum of the times associated with all the states during a given measurement period.

If $m$ is the total number of unique states in the system, and $\pi_k$ is the number of occurrences of state $k$ over the entire measurement period, then the “rate” of occurrences of a given state during the measurement period, $q_k$, is given as:

$$q_k = \frac{\pi_k}{time \ in \ state \ k}$$  (1)

The significance of $P_k$, $q_k$, and equation (2) will be developed in the next section.

B. Probability, Entropy, Energy, and Temperature

Once a probability measure is assigned to a state the system entropy is determined by computing the partial statistical entropy for each individual element and then summing all of the partial entropies to achieve the system entropy during a discrete measurement period, $t$, as shown in equation (2) ([7]):

$$\text{entropy}_t = \sum_{k=1}^{m} P_k \ln P_k$$  (2)

The state-based statistical nature of this system, where transitions between states may take place at any instance of time, can be represented as a continuous time Markov chain. In this case, $q_k$ represents the rate of transition through state $k$ and the generator of the process, $Q$, is a function of the discrete transition probability matrix associated with the Markov chain [8].

In the form of Maxwell ([9]), $P_k$ can be alternatively represented as:

$$P_k = e^{-\frac{H_i}{T}} = e^{-\frac{H_j}{T}} = e^{-\frac{H_{ij}}{T}}$$  (3)

and in keeping with the traditional notation in statistical mechanics refer to $H_i$ as the energy of the $i^{th}$ state and $T$ as the system temperature. If we carefully choose the state assignments such that the “center of mass” of the state energies sum to zero, we can find $H_i$ by:

$$H_i = T \ln \left( \frac{\prod_{j=1}^{m} (P_j)^{\frac{1}{m}}}{P_k} \right)$$  (4)

In practice, the numerator rapidly approaches zero and must be appropriately scaled by applying an exponentiation of $1/m_i$ to the final numerator product in order to ensure computationally valid values. This scaling produces equation (5), which more accurately reflects the internal formula used in the Therminator process:
Energy depends on the summation of the individual state’s energies, or $H_i$, weighted by the probability associated with that state. The total energy of the system can thus be described with equation (6):

$$
\text{energy}_i = \sum_{k=1}^{m_i} (P_k H_k)
$$

Computing system temperature is a great deal more complex. The basis for temperature is a transformation function comparing the state progression of the current measurement period with the state progression of the previous measurement period and then relating the previous temperature to the new temperature via this transformation. This sets up a recursive relationship for temperature that behaves as detailed in the equation below, where $\varphi$ is the transformation function.

$$
T_0 = 1 \\
T_t = \varphi T_{(t-1)}
$$

Making the substitutions into the above equations, the temperature at time $t$ can be calculated using the following equations:

$$
T_0 = 1 \\
M_0 = 1 \\
T_t = T_{(t-1)} \left( \frac{M_t}{M_{(t-1)}} \right)
$$

C. Graphical Display of Conversation Flux: The Thermal Canyon

Figure 3 illustrates the components of the graphical display provided by the Therminator program. In the upper left hand corner is the window containing a graph of the computed entropy, energy, and temperature. The upper half of the main window, sometimes referred to as “Thermal Towers”, shows the average number of balls in a bucket for a given period of time, while the lower half of the main window, referred to as the “Thermal Canyon,” shows the sorted state counts produced during a measurement period.

The curves produced when ranking the states by their counts is analogous to the Boltzmann curves of probability versus energy state of molecules in a gas [6]. Using the Boltzmann analogy, the area under the Therminator state curve is a proportional representation of the temperature, while the slope of the state curve becomes a proportional representation of the entropy, and the change between time slices or slides becomes a proportional representation of macroscopic energy fluctuations. Changes in thermal canyon represent heat in or out of the system. Changes in network configuration reflect work done on the network by the outside world or work done on the outside network by the defended network.

By examining the manifold, or canyon, developed by collecting various curves over time, anomalies can be easily spotted as perturbations in the normal flow of the canyon. Normal flow varies from network to network as well as time scale and coarsening level employed in creating the bucket descriptions. Although often evident in a graphical sense, a mathematical meaning of “normal” is still under development. Throughout the canyon there should be thermal equilibrium as well as anomalous ebbs and flows (the equilibrium fluctuations typically accompanied by symmetric entropy fluctuations), since the primary orientation of network traffic changes over time. At one instance the majority of network traffic may be monopolized.
by a large file transfer characterized by a small number of large packets, and within the next segment of time the traffic may be monopolized by an SNMP network poll characterized by a large number of relatively small packets. The Boltzmann curves for either of the above instances would look similar in shape but perhaps are scaled with respect to one another, possibly along the time axis, state axis, and/or probability axis. What signals an anomaly is a rather abrupt change in the various ebbs and flows. The cause of such dramatic changes in practice ranges from a single transition to many thousands of packets. The next section details some of the analysis results seen during development testing.

3 Implementation And Observations

The present manifestation of Therminator was designed for IP networks. Bucket assignment may be determined by any of the following conditions: matched reply, flow direction, a previously unseen IP address, IP and/or TCP header length, protocol type, packet size and broadcast indicator. The definition of a bucket space depends entirely on the network being monitored and often requires some trial-and-error testing to develop a suitable set of conditions. Typically, three conditions (eight buckets) would be used with 20 balls.

This system has been tested at the egress point of three operational networks. Typical traffic loads ran between 3000 – 5000 packets per second. Some observed phenomena are described below.

A. ICMP Anomaly Example

Figure 4 depicts a flood of ICMP packets originating inside the monitored network after normal working hours. This flood increased the state count; thereby producing a large spike on the GUI. This flood consisted of 6,032 ICMP echo requests/replies within a ten second time frame. ICMP echo requests and replies are not necessarily anomalous, however the owner of the system was logged off and at home requiring notification of the local CERT for further investigation.

An important point to note, Therminator was the only system that captured this event. The administrators of the monitored network heavily depends on two commercial intrusion detection systems, and neither system caught the event. The only proof that helped verify the event actually happened was a router’s logs.

4 Conclusion

We have presented a system for characterizing the dynamics of conversations occurring across a boundary of an organization’s network. This system appears to have significant potential for monitoring the health of networks as well as intrusion detection. The system is modeled after statistical mechanics methods for developing notional trends from large volumes of data.

This system has been observed operating in real network environments and has produced some intriguing results. Specifically, the system has been shown to detect phenomena that are not detected by any other network sensor. While not always an indicator of malicious activity, this has proven to be a significant resource for network administrators as an aid to understanding how their network is being used.

We acknowledge the need for Therminator to partake in a structured test. We are actively pursuing the development of a test environment in the vein of [10], to advance our understanding of Therminator’s capabilities and validate its outcomes.

Finally, we are also currently evaluating methods for systematic definition of a bucket space based on the use and function of the network to be monitored. Presently the bucket space is defined through trial-and-error, resulting in time consuming and often inefficient use of resources.

REFERENCES

Figure 1. (Left) An example of a state walk starting with 5 balls in each bucket. (Center) A table of the transitions for each bucket. (Right) The distribution of balls in buckets for this state walk.

Figure 2. (Left) An example of a second state walk also starting with 5 balls in each bucket, however, a completely different trajectory is taken. (Center) The table of transitions for each bucket. (Right) The distribution of balls in buckets for this state walk. Note the significant difference from the right hand side of figure 1.

Figure 3. 3-D Graphical User Interface of Network Analysis Tool Developed in this paper.

Figure 4. ICMP Anomaly Example – The red perturbation was a series of 6,032 ICMP packets sent in a span of ten seconds.