

# Therminator

## A transformational enabler for FORCEnet

By John McEachen, John Zachary and David Ford

“Slammer, Blaster, Code Red” — the simple fact that the general public associates these terms with computer network attacks speaks volumes for how far awareness of network security has advanced in the past few years. Unfortunately, the same cannot be said for the technology designed for repelling these attacks. Change has been incremental and, for the most part, we are still conducting business the way we were 20 years ago. Consequently, while the sophistication and virulence of network attacks have increased exponentially, the ability to stop these attacks has advanced only linearly.

For example, in 2001 Code Red infected over 300,000 network hosts in half a day. In 2003, it took under 30 minutes for the Slammer worm to infect over 75,000 hosts, 90 percent of which were infected in under 10 minutes. This escalating rate of propagation highlights the requirement for network detection mechanisms to serve as real-time early warning devices. Clearly, there is a critical need for transformational change in the way the Department of Defense (DoD) performs computer network defense (CND).

Therminator is a new and radical approach to CND on an immediate basis and to systems of exchange on a more abstract level. Consequently, Therminator is well-suited as a transformational enabler for

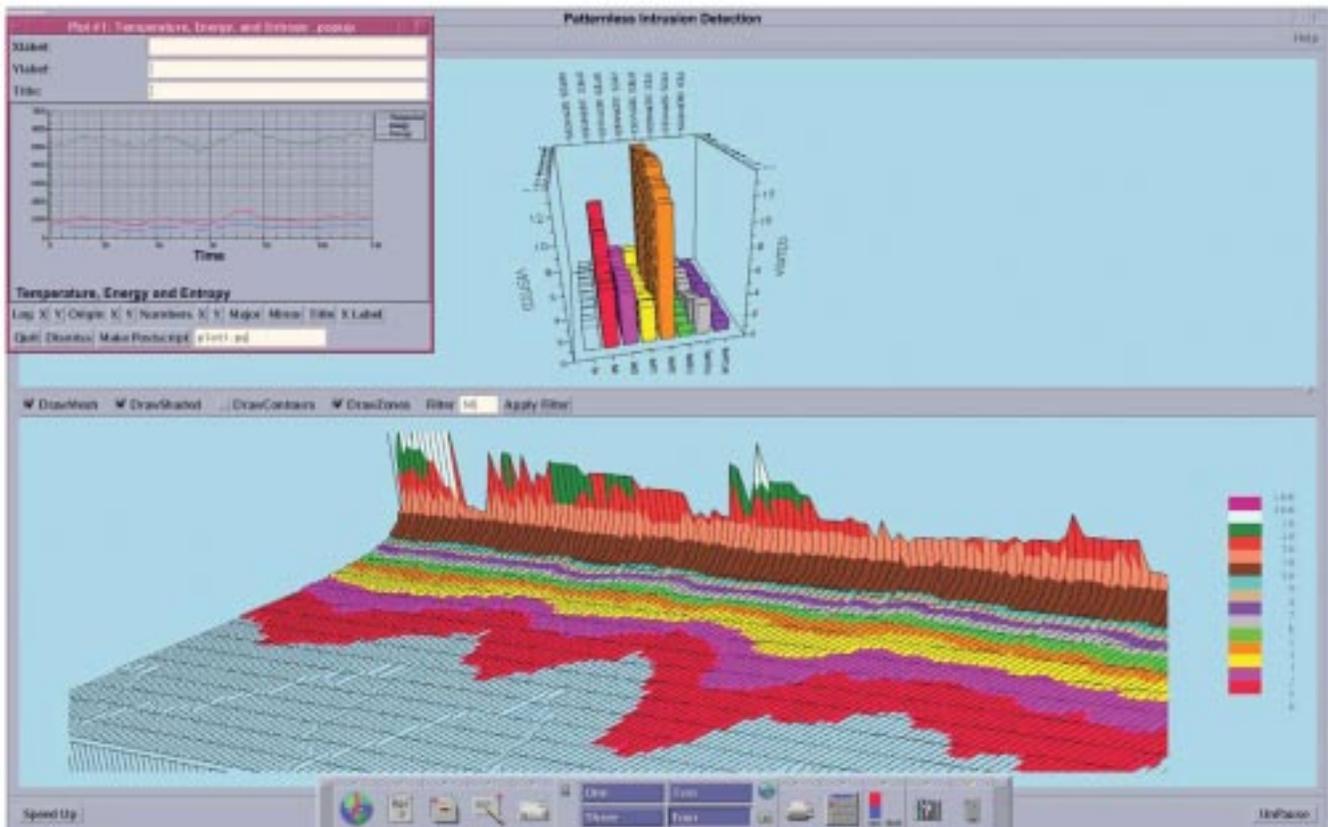
the network-centric vision of FORCEnet. While the specific application of Therminator has been most recently applied to IP networks, the concepts and techniques can be applied to all manner of networks and communications systems.

Therminator is based on proven science from combinatorics, statistics and thermodynamics. The system can be considered a new layer in the “Defense in Depth” approach to network security and provides network administrators with a novel perspective (Figure 1) on how their network is operating. Therminator is highly scalable and its composite approach can even facilitate creation of “Therminators of Therminators.” It has been tested at the U.S. Pacific Command Network Operations Center, Ft. Shafter, Hawaii, U.S. Pacific Command Headquarters, Camp H.M. Smith, Hawaii and the U. S. Army Signal Command, Ft. Huachuca, Ariz. Follow-on installations are being planned.

### Background

The development of a dependable and secure networked computing infrastructure depends on real-time monitoring and detection of anomalous events. These events and behaviors typically are sourced at a host and are propagated over a network to a victim

Figure 1. A generic snapshot of the primary Therminator display. The top portion of the graph is a display of average bucket sizes associated with conversation groups. The lower portion of the graph illustrates the “thermal canyon” — the relationship of various network states over time (indicated from left to right).



host or network. The typical approach is to apply intrusion detection principles to a network to capture and classify malicious behavior. The earliest intrusion detection systems (IDS) integrated signature-based analysis for detection with normal network models. Since then, many different systems have been based on the assumption that malicious network activity is inherently different from normal activity. Recent experience, however, suggests that the scope and character of network attacks is such that intrusion detection systems are insufficient network protection mechanisms. This is especially true of signature-based IDS, which compare real events to a set of known malicious or abnormal events. These types of systems are poor at detecting new attacks, variations of known attacks or attacks that can be masked as normal network behavior. The complex, interactive nature of computer networks is subject to the critical mass effect. The spread of worm-like attack is much like the effect observed with a paper napkin when increasing force is applied. The progress of the tear is hardly noticeable at first until, quite suddenly, the napkin is ripped in two. The physical nature of complex, interactive systems such as computer networks highlights the need for rapid, real-time indication of attack propagation.

Thus, there is a real need for a new approach in thinking about CND. Therminator emphasizes active real-time network monitoring and anomaly detection as complementary mechanisms to the traditional network intrusion detection process. The separation of network traffic behavior into normal, anomalous and malicious categories under the umbrella of real-time monitoring and configuration management gives operators a holistic view of network activity.

Motivated by the need for CND transformation, the real-time implementation of Therminator was developed in 2001 at the Fort Shafter NOC by two students of the Naval Postgraduate School, Lt. Stephen Donald, USN, and Capt. Robert McMillen, USMC. Using live operational network traffic and working in tandem with scientists from the National Security Agency, the Institute for Defense Analysis and the SANS (SysAdmin, Audit, Network, Security) Institute, the team produced a working application in 90 days. Testing and analysis have continued over the past two years and in March 2003, software development was picked up by the University of South Carolina Distributed Systems Security and Cryptography Laboratory.

Most recently, Lancope, Inc. of Atlanta, Georgia, released a version of its Stealthwatch Intrusion Detection System that integrates many

of the Therminator concepts. This product, called Stealthwatch + Therminator (SW+T or SWAT), combines the information-dense yield of Stealthwatch with the data reduction features of Therminator to produce a system that provides both macro- and micro-views of an IP network. The ideas behind SW+T are based on a non-exclusive license purchased by Lancope from DoD in November 2002.

Commercial ventures notwithstanding, research in Therminator applications aligned with specific national security interests continues at the Naval Postgraduate School, the University of South Carolina and the Georgia Institute of Technology. Areas of investigation include implementation of Therminator in hardware to operate at gigabit speeds, and analysis of Therminator concepts in nontraditional networks.

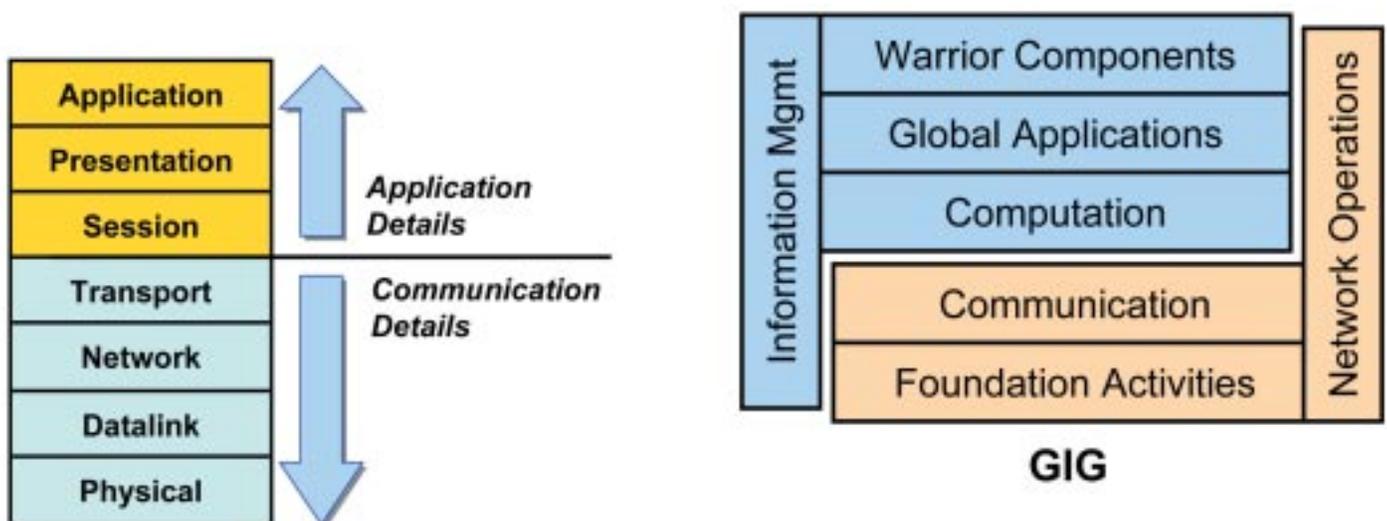
### Concept

A computer network is a complex interactive system. The signal it produces is the result of many millions of precise, directed exchanges between thousands of its component parts. To maintain information superiority, survivability (reliability, usability and security) and mission support, it is essential that the state of readiness in this complex machine be timely and understandable to decision makers at several levels in the chain of command. In addition, it is crucial that this trusted state of readiness be defended from those that continually act to undermine both its readiness and integrity. This means that the long and short term actions of those who seek to control our critical infrastructure be transparent to those entrusted with the task of defending and repairing it.

For many researchers the complexity of this problem is an obstacle. The Therminator research initiative uses the complexity of this problem as an advantage. By extending the work and lessons learned by many generations of scientists, Therminator uses the well-founded theories of statistical mechanics and combinatorics as a template and a strategy for dynamic data reduction, visualization, analysis, interpretation and forensics. Thus, it does not rest on the ad hoc opinion of a single researcher or single group of researchers on what seems like a good strategy, it avoids reinventing the wheel by building on well-established scientific and mathematical principles.

Therminator provides a continuous real-time, compact and visual representation of states of exchange between network entities. The basic premise results from modeling the network as a finite number

Figure 2. The division of labor in the Therminator model. Therminator provides a general mapping of the characteristics of communications exchanges, providing a generic metric for warfighters to compare anomalies across applications.



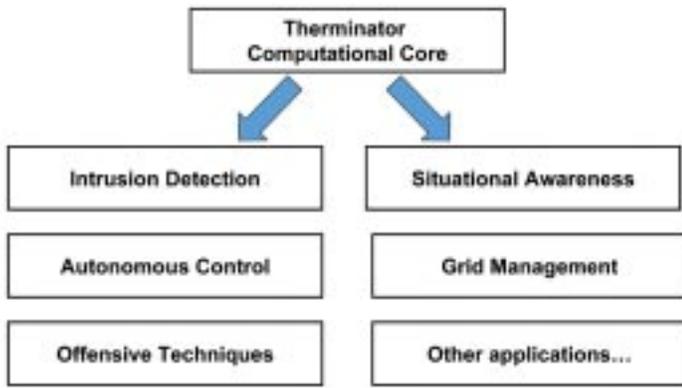


Figure 3. Therminator's approach can be applied across a broad spectrum of FORCEnet applications.

of conversation groups called buckets that pass information, called balls, among themselves. This produces a notion of a network state represented by the aggregate of all the buckets with the balls they contain. The complexity and asynchrony of this exchange among a large set of network nodes creates a high-dimensional combinatorial system to which dimensionality reduction inspired by statistical physics is applied. From this network state and the state transitions that occur during each packet arrival, the thermal properties of entropy, energy, temperature, work and heat can be computed and displayed. Asymmetrical perturbations in these displays have revealed anomalous network activity resulting from malicious activity and misconfigurations, some of which were not detected by standard signature-based intrusion detection systems.

### Application to FORCEnet

Computer networks and interacting systems in general, are based on a layered architecture to facilitate systems interoperability and design. The layered design paradigm permeates many modern distributed systems affecting solutions to the association problem.

The inherent elegance in the Therminator approach and the aspect that makes it applicable to FORCEnet, is that it yields a model of conversation exchange dynamics that is consistent across horizontal levels (different applications) and across vertical levels (different architecture layers, shown Figure 2). A consistent model across vertical levels will allow technicians, analysts and decision makers to compare apples to apples because all behavior is cast in the same general model (conversation exchange dynamics). This will reduce the time from data collection to information creation to knowledge understanding and finally decision making.

In other words, using the Therminator approach, anomalous activity in one environment (e.g., satellite control systems) could be reliably correlated with activity in a very different setting (e.g., IP networks). This is made possible because both are considered only in terms of their exchange properties and related dynamics. A subset of these potential applications is shown in Figure 3.

The Therminator architecture as shown in Figure 4 is based on an application-independent central core processing element that is fed by application-dependent sensors. In the case of IP networks these sensors are packet sniffers which perform rudimentary metadata association. External to the core are the graphical user interface (GUI) modules and plug-ins for second-order analysis of the core output.

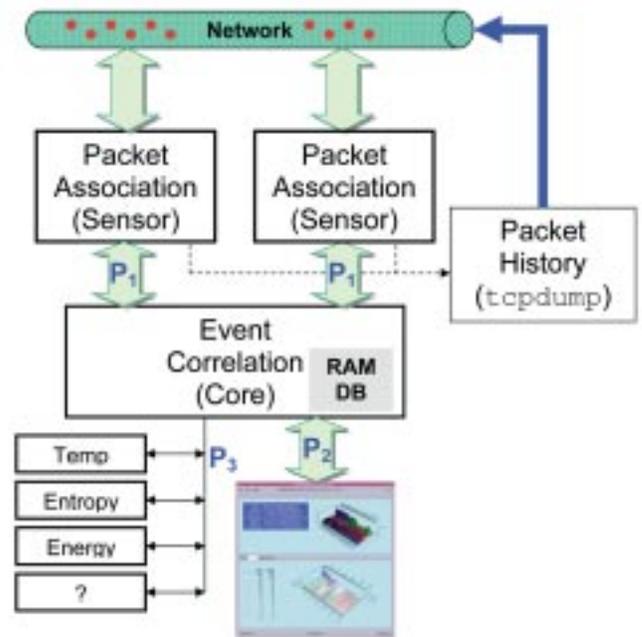


Figure 4. The Therminator architecture is centered upon a core event correlator. Input is received from application-dependent sensors and output is fed to a GUI and second-order plug-ins.

### Examples

Therminator has been extensively tested in both controlled laboratory settings and on real-world network traffic. The current software-based implementation handles generated network traffic from 10 Mbps to 100 Mbps without dropping packets. A visualization of the bucket spaces and thermal manifolds provide interactive real-time feedback of the conversations exchange dynamics. Users are able to drill-down to specific packet information simply by clicking anywhere in the GUI.

Figure 5 illustrates the thermal manifold or "thermal canyon" produced from an exchange between 1,000 client machines on an untrusted network with 10 Web servers on a trusted network. Network load was approximately 1,500 packets per second. Figure 6 illustrates the same exchange of traffic with a single UDP (User Datagram Protocol) packet injected. The difference in the thermal canyon between Figures 5 and 6 is evident, keeping in mind that during this two-minute period over 200,000 packets were exchanged.

Figure 7 shows the Therminator response to an actual event on an operational network: a flood of ICMP (Internet Control Message Protocol) packets originating inside a monitored network detected after normal working hours. The packet flood consisted of 6,032 ICMP echo requests/replies within a four-second time period. ICMP echo requests/replies are not anomalous per se. In this event, however, the owner of this particular client machine was logged off and at home, thus prompting a notification to the local CERT (Computer Emergency Response Team) for follow-up. This event was not detected by any other installed network protection system.

The final example of an operational success of this model occurred when Therminator detected a Code Red worm attack during a demonstration. The case study shown is an interesting example of the range of anomalies that Therminator is capable of revealing. Figure 8 shows a small number of packets entering the NPS network that correspond to the Code Red worm. This is in contrast to the result of the swift counteraction of the firewall administrator shutting

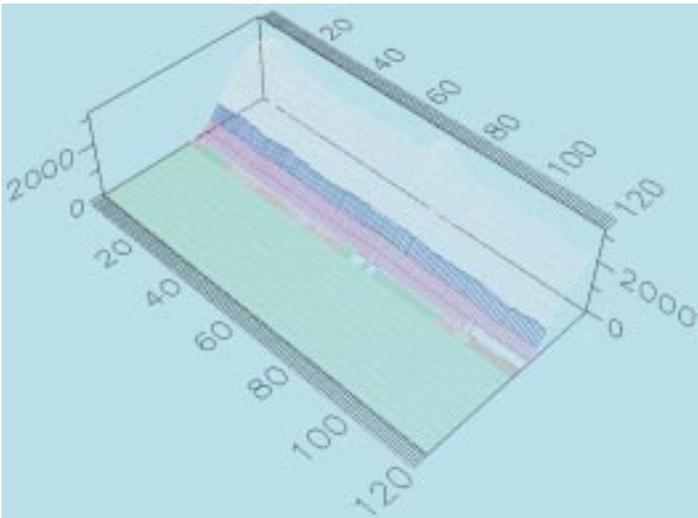


Figure 5. The display associated with synthetic network traffic from 1,000 untrusted clients to 10 trusted Web servers over a period of two minutes. This figure represents over 200,000 packets.

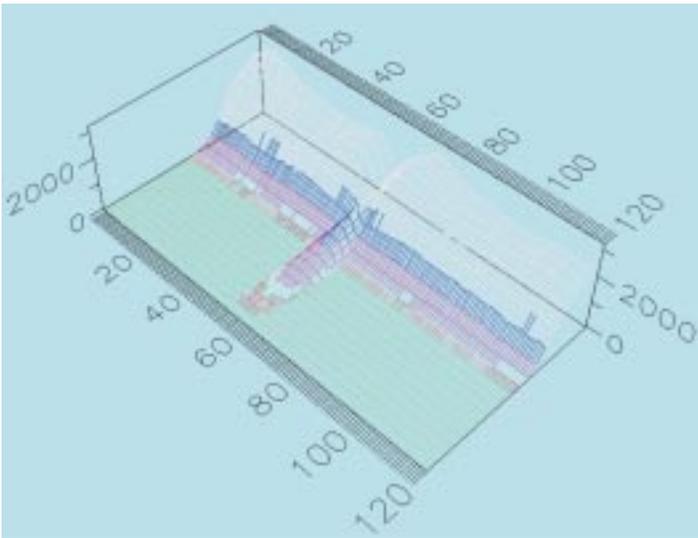


Figure 6. The same 200,000 packets shown in Figure 5 plus a single additional UDP packet. The difference is evident at approximately 60 seconds.

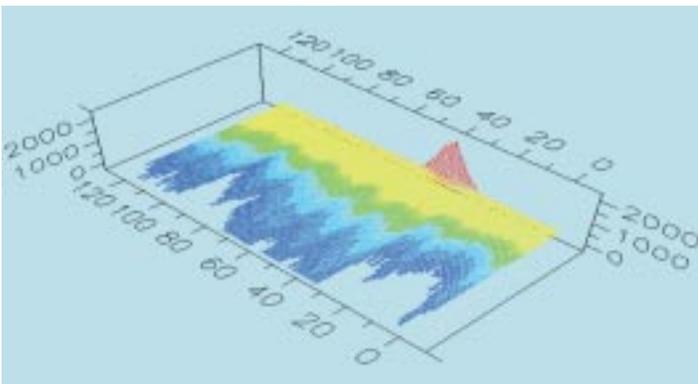


Figure 7. A snapshot of an actual packet flood observed within an operational network. This flood consisted of over 6,000 packets in a four-second period from a single host during off-hours.

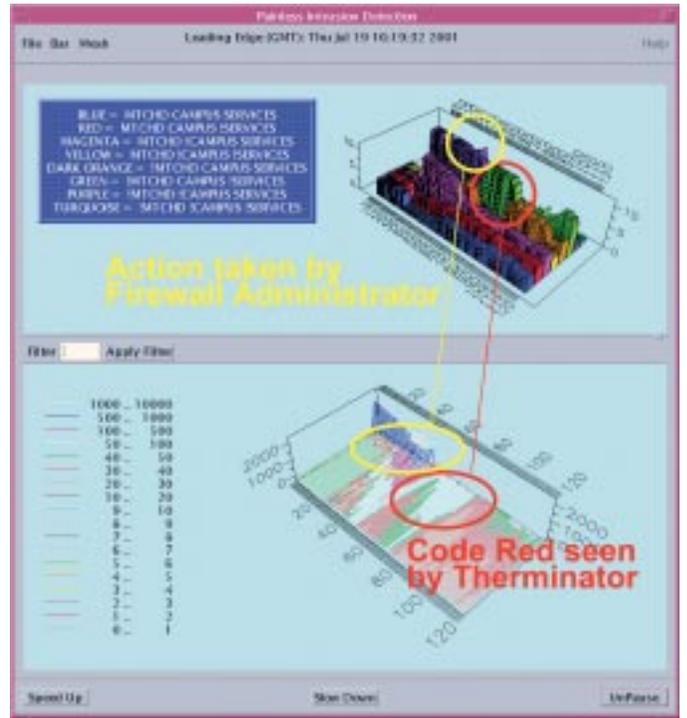


Figure 8. A snapshot of the Code Red attack in progress. The display highlighted by the red circles is associated with the Code Red worm entering the NPS campus. The area highlighted by the yellow circles is associated with the firewall administrator shutting down the firewall in response to notification of the arrival of the worm. Compare the display associated with the intrusion of the Code Red worm with that of the actions taken by the firewall administrator shortly thereafter.

down the firewall highlighted by the yellow circles. This area shows thousands of Web requests heading to the Internet while all the responses are blocked.

## Summary

Therminator is a radical attempt at transformation in DoD CND and in FORCENet monitoring in general. Traditional approaches to CND cannot keep up with the rapid changes in network intrusions. By reducing data to an expression of exchange dynamics, Therminator can provide a metric for an apples to apples comparison across communications applications thus allowing for informed and rapid decision making.

*John McEachen is an Associate Professor of Electrical and Computer Engineering at the Naval Postgraduate School. Dr. McEachen is the co-director of the ECE Advanced Networking Laboratory and the former director of Reconfigurable Intrusion Detection and Deception Laboratory Research (RIDDLR). In 2003, he was awarded the Richard W. Hamming Award for excellence in interdisciplinary teaching and research.*

*John Zachary is an Assistant Professor of Computer Science at the University of South Carolina and Director of the Distributed Systems Security and Cryptography Laboratory. Dr. Zachary was formerly employed by the Advanced Research Laboratory of Penn State University.*

*David Ford is a Research Professor at the Naval Postgraduate School and the DISA chair for Information Assurance. He is formerly of the National Security Agency.*