Intrusion Behavior Detection Through Visualization

Robert F. Erbacher
Department of Computer Science, LI 67A
University at Albany-SUNY
1400 Washington Avenue
Albany, NY 12222, USA
erbacher@cs.albany.edu

Abstract - *As computer and network intrusions become more and more of a concern, the need for better capabilities to assist in the detection and analysis of intrusions also increases. We propose a methodology for analyzing network and computer log information visually based on the analysis of user behavior. Each user's behavior is the key to determining their intent and overriding goals, whether they attempt to hide their actions or not. Proficient hackers will attempt to hide their ultimate goal, which hinders the reliability of log file analysis. Visually analyzing the user's behavior, however, is much more adaptable and difficult to counteract. This paper will discuss how user behavior can be exhibited within the visualization techniques, the capabilities provided by the environment, typical characteristics users should look out for (i.e., how unusual behavior exhibits itself), and exploration paradigms effective for identifying the meaning behind the user's behavior.*

Keywords: Intrusion Detection, Visualization, Computer Forensics, and Behavior Characterization

1 Introduction

Intrusions and misuse of computer systems are becoming a major concern of our time [6], [2]. Our nation's infrastructure is heavily network based in all industries. The nation's infrastructure is not capable of dealing with attacks on a local or global scale, leaving network and computer security up to an organization's individual efforts. Intrusion and misuse detection, however, has proven to be an extremely difficult problem to tackle. Techniques have applied signature-based techniques (snort [8]), heuristic-based techniques, data mining, neural networks, visualization, etc. [1]. Techniques can either be geared towards affirmative or negative results. Techniques geared towards affirmative results are designed to activate an alert when a pattern sufficiently matches known attack criteria. Negative result techniques are geared towards providing an alert when the pattern does not match any known or expected pattern. This is indicative of anomalous or questionable user activity. In either of the two cases the techniques are essentially geared towards identifying a pattern of activity deemed to be questionable in nature. This pattern of activity is indicative of the user's behavior.

This attempt to analyze a user's behavior is critical to intrusion and misuse detection. No matter what techniques are applied to identify intrusions and misuses, the end result is that the system administrator or security expert must perform an examination of the user's behavior to determine the goals and intent of the user. All available techniques are limited in that they generate high false positive and false negative rates. These false results must then be examined to determine their true nature. In essence, this becomes a question similar to that seen in the forensic sciences: Why did the user do that? Is this an attempt at malicious activity or is it innocuous? Much of this analysis can be done through the available data. Some of this analysis must be done in concert with the user through queries to identify their goals; as is done through typical forensic processes. Consequently, computer forensics [7], the process of analyzing the data, is critical to the effectiveness of the intrusion analysis process.

2 Goals

New capabilities are needed to aid the behavioral analysis aspect of intrusion and misuse detection. The typical techniques we mentioned previously will provide an initial indicator if something unusual occurs. However, what does it mean that this unusual event occurred? We are proposing visualization capabilities to aid in the analysis of the highlighted activity [5], [4]. The goals of these techniques are to aid in answering the questions that arise when anomalous activity is identified:

- Why did the user do that?
- Is this activity really indicative of an attack?
- Is there a reasonable explanation for why the user did this?
- Has the user behaved unexpectedly in the past?
- Is this activity typical for other users?

Additionally, the visualization techniques by their very nature aid us in analyzing the behavior of individuals, behavior that under normal circumstances would be

0-7803-7952-7/03/$17.00 _ 2003 IEEE

completely missed. This relates to our added ability to correlate activity both spatially (on different machines) and temporally to derive a greater understanding of what is occurring on the network. For example, we can correlate activity for a single user over an enormous period of time, even weeks, with the visualization environment. Without the visualization environment, say if the administrator was relying on the original text-based logs, then an enormous amount of time would be required to correlate events that are either temporally or spatially disparate. Ultimately, the goal is to provide a better, more complete understanding of the behavior indicative of a user or system such that the behavior can be more fully examined and analyzed.

3 Visualization

Ultimately, our goal is to provide a complete exploratory data analysis environment to aid in the analysis of the data available to the system administrator. We are looking to incorporate both raw data, e.g., system log files, system statistics, and network traffic data, as well as computed data, e.g., alerts generated by portsentry, snort, and other intrusion detection tools. These data parameters will be represented visually within the visualization environment by mapping them to visual attributes through the use of glyphs [3]. Glyphs can be conceived as generalizations of pixels that allow many data parameters to be mapped to a single visual element, providing for the representation of highly dimensional data. Additionally, we incorporate multiple visual representations, as a single representation is never sufficient to analyze all aspects of the data. These multiple representations are in effect coordinated views of the data set, allowing the same data to be examined and analyzed in different ways. By having the views coordinated, we can identify an element of interest in one display, select that element, and observe it highlighted in all other displays. Currently, we incorporate an animated, glyph-based visualization, a simple line-based histogram visualization, and a pixel-based histogram.

In order to provide the exploratory capabilities we are incorporating extensive interaction. It is through these extensive interaction techniques that we will provide the forensic analysis capabilities to examine and eventually comprehend the meaning of the user's activity. The visual display itself provides abstractions and generalizations. In order to retrieve specifics we provide probing and feedback mechanisms. This provides the specifics needed to fully understand the meaning behind the data. Additional interaction capabilities provided include:

- **VCR like controls.** These controls allow the animated visualization environment to be sped up, slowed down, and paused. This allows the user to focus on periods of activity for greater analysis.
- **Element selection.** In addition to retrieving detailed specifics on an element, we can select an element to highlight it. This allows the element to be followed or monitored over time. With the coordinated views we need only select the element in one display to follow it in all displays.
- **Go to time command.** When a time of unusual activity is identified in one of the unanimated displays, this command will allow the environment to jump to the selected time. This allows greater attention to be focused where it is needed.

The resultant capabilities not only allow the user to identify what happened but potentially why, when, and where? Answering the critical forensic questions that are intrinsically dependent on the analysis of the behavior of the individuals under examination.

4 Behavior Characterization

When attempting to analyze and comprehend an individual's behavior we must consider the meaning of typical behaviors such that when unexpected behavior is identified it can be categorized based on similarity to other activity. Additionally, similar sets of actions can have vastly different meanings depending on which commands are used and the nature of the environment. For example:

1. Is a remote user connecting directly to a local workstation rather than to the server acceptable?
2. Is a user executing the same command over and over again acceptable?
3. Is it acceptable for a user to connect to multiple machines simultaneously or connect *through* machines to others?
4. Is it acceptable for one remote machine to be connected with multiple logins or user names?
5. Is it acceptable for a single user to consume a majority of a resource on a system, whether it be disk space, CPU time, or network bandwidth?

When considering these different scenarios they each clearly have different characteristics. Thus, when examining similar behavior we can identify the category it matches which will in turn identify what additional specifics must be looked at to discern grater meaning behind the behavior. This list is by no means complete but is designed to show examples of the types of activity to be examined, which will vary among organizations.

For instance, the impact of the first scenario will be greatly dependent on the rules and configuration of the network environment. If, for instance, the environment were configured to allow remote connections only to a single dedicated host, perhaps a firewall, then such activity would be considered to be unacceptable. Other systems may be designed to only allow select individuals to connect at all, e.g., members of a lab.

In the second scenario, the command that is being executed is critical to identifying its underlying meaning. An individual entering the 'ls' command over and over again will in general be harmless. Similar behavior with the 'w' command would be considered anomalous and is in fact considered to be the behavior of an intruder. Intruders use the 'w' command to ensure they are alone on the system and not being monitored.

Why would a user need to connect to multiple machines when a single machine will generally suffice? In specific cases this may be a necessity, e.g., development of networking code. However, in general, most individuals would not need to behave in this manner and thus it can be considered anomalous until shown otherwise.

Depending on the type of system acting as the remote host, it is quite possible to have multiple individuals validly connecting to a local machine from that same remote host. For example, many students within the Computer Science Department may connect from the department's server to the university's server. This would be far more unusual with a system not localized to within the university. Such behavior can be indicative of compromised accounts. This is similar to identifying individuals who change their userid from one student account to another. Why do they have access to multiple accounts? At the very least this is an abuse of the account system.

Finally, use of large amounts of resources would be considered anomalous, especially in conjunction with other anomalous activity. For example, if a user connects directly to a workstation instead of to a server and begins consuming large amounts of CPU resources it is reasonable to identify *what* is being computed. It is often the case that password crackers are run on idol workstations with the user running the 'w' command frequently to ensure they are not noticed; thus multiple anomalous behaviors in coordination. Identification of one anomalous act should lead to the analysis of additional data to identify other anomalous activity.

5 Visual Behavior Analysis

As can be seen from the previous section, there are enormous implications of behavior on the meaning of an individual's actions. Identifying the behavior behind such activity is the application of the forensic process. The difficulty with this process is its time consuming nature and the need to examine enormous volumes of data in order to derive this information. For example, monitoring connection information would require monitoring at least tens of megabytes of data per day and identifying disparate correlations. This correlation of activities is one of the principal problems with intrusion detection and monitoring. This connection-based information can be derived directly from system log files. Additional information is available from the kernel directly and from network traffic data. The need for these sources of data are exemplified from the following examples:

- One of the principal goals of an intruder after gaining access to a system is to compromise the log reporting facility. Thus, the system log files can become unreliable. Collecting and monitoring network traffic data can identify such irregularities. However, monitoring network traffic data itself brings its own difficulties, particularly in relation to the volume of data.
- We identified previously that identification of the frequent use of the 'w' command could identify the behavior of an intruder attempting to remain undetected. However, what is to keep a user from changing the name of the command? By monitoring kernel level calls, the *behavior* of the 'w' command can be identified even though it may be renamed or obfuscated in other ways.

Thus, it is important not only to discern the behavior of the user but also the behavior of the individual commands they are attempting to use.

Given the volume of available data, our goal has been to apply visualization techniques to the intrusion detection and analysis process. Visual analysis of behavior has proven critical to this step. We have developed several visualization techniques geared towards this process.

5.1 Animated Glyph-Based Visualization

First, we have developed an animated visualization technique. This visualization technique maps data parameters from system log files and associated system statistics (system load, number of users, and disk space consumed) to the elements of the glyph (Figure 1).

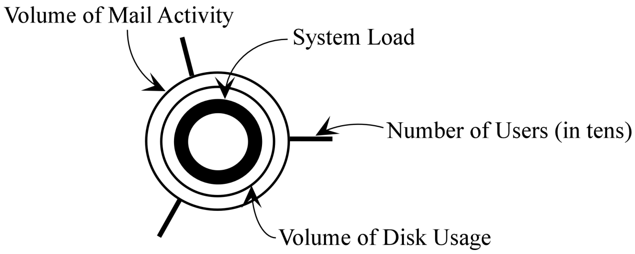

Figure 1: Example host-based glyph for the animated visualization technique. Connection information is added as line-based glyphs. Data parameters are mapped to the visual attributes. Additional parameters can easily be added.

Lines show connection information from remote nodes to local nodes. The line style indicates the type of connection:

- Two parallel lines – initial inetd
- Single solid line – telnet, rlogin, shell
- Single long dashed line – privileged ftp
- Single short dashed line – anonymous ftp
- Single solid line with multiple arrows – NFS
- Two parallel red lines – failed connection
- Single thin red line – failed authentication
- Single thick red line – portsentry message

Additional formats can easily be added. By monitoring this animated representation we can easily identify and correlate activity (behavior), that otherwise would be obfuscated within the deluge of data generated by the network each day. For example, unusual system loads are clearly identified, as are individuals connecting to multiple machines, users connecting remotely to workstations, users connecting *through* one machine to get to another, a single remote machine connecting to multiple machines, either simultaneously or in rapid succession, etc. When animated, these characteristics take on particular clarity and each is indicative of behavior requiring additional analysis.

5.2 Histogram-Based Static Visualization

The histogram is a simple line-based visualization that provides a mapping of event severity (Y Axis) versus time (X axis). In any environment, there will be sporadic activity identified as having a higher severity than other events. This technique allows unusual activity to be identified, whether it is grouped events of high severity or a single host (or user) with unusual sequences of severe events. In essence, the user mode highlights user behavior and the host mode highlights host behavior. A subset of the severity levels for different events is shown in Figure 2.

Syslog Identifier	Numerical Value
ALERT	9
ANONYMOUS	5
INETDFTP	2
INETDTELNET	2
LOGININCORRECT	8
PORTMAP	7
PORTSENTRY	10
PRIVILEGED	2
SUDO	10
TELNET	2

Figure 2: A subset of syslog identifiers and their associated severity levels, as an integer in the range of 0..10. Entries can be changed or additional entries added by editing the text-based file containing the associations.

The histogram-based representation is enhanced by allowing both host-based and user-based views. Clearly, since most severe events are by unknown users (e.g., portsentry identified portscans) the host-based view will include far more data than the user-based view. Second, by selecting a user or host, that entities entire activity over time is highlighted and can be examined, allowing for greater analysis of that entities behavior.

5.3 Glyph-Based Static Visualization

The glyph-based static visualization (i.e., a pixel-based histogram) technique is geared towards reducing the limitations of the histogram-based techniques, particularly the amount of occlusion that occurs. The glyph-based visualization again represents the severity level, though in this scenario as a green → red scale. Additional information is overlaid on top of the severity scale. An example is shown in Figure 3.

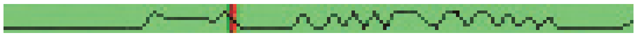

Figure 3: Example glyph-based static visualization. Connection information is overlayed on top of the green → red scale as a line-based histogram.

As can be seen from this example, we are overlaying connection information as a histogram. In the host-based mode we have one line for each remote host. The host this system is connecting to is represented by the histogram. Similarly, for the user-based mode we have one line for each user and the histogram represented the remote host the user is connecting from or the local host the user is connecting to. The key here is to identify changes in user behavior. If a user only connects from one host all the time but suddenly changes their behavior and connects from a different host then this should be noted and a reason identified. The reason can be innocuous such as a student graduating or going to a conference. On the other hand, it could be a compromised account and an intruder connecting from the remote host. Identification of additional information surrounding the activity is critical towards fully analyzing and comprehending such changes in behavior. However, resolution of such anomalies is critical if intrusions and misuses are to be identified and resolved before more substantial damage is incurred.

5.4 Exploratory Data Analysis

The visualization techniques developed are only the first step in the process. Our further goal is to aid the analyst in identifying the meaning behind given activity. Is it truly an attack or is it merely random behavior. Determining this greater meaning requires facilities within the environment to explore the data and analyze it in greater detail than can be presented within a single display. Thus, the need for the exploratory data analysis capabilities mentioned previously. The ultimate goal is to limit the analysts need to rely on the original raw data, as the reading of textual data is prohibitively expensive in terms of the data analysis performance in contrast to the use of the visualization techniques. Such capabilities include:

- The ability to probe a host and retrieve its hostname, IP address, and the usernames of each individual connecting from that system.
- The ability to select a host in one visualization technique and have it highlighted in all visualization windows (coordinated multiple views).
- The ability to highlight a node and follow it over time.
- The ability to interactively go forward and backward through time at a user controlled rate. Thus, allowing careful analysis of critical information and time periods.

6 Examples

The discussed techniques have proven effective in the identification, analysis, and exploration of anomalies. The goals are to speed response time and improve attack analysis. This requires allowing the analyst to quickly identify false positives and false negatives such that they can be removed from consideration. Below we provide examples for each of the visualization techniques.

6.1 Histogram Visualizations

As an example of the need for behavior analysis, consider the line-based histogram shown in figure 4. In this example, we have a tight cluster of many high severity events. When such activity is encountered the question as to whether this is an attack must be raised. If the system administrator had to rely solely on the textual data then this unusual behavior would likely have been completely missed, allowing a potential attack to go unchallenged.

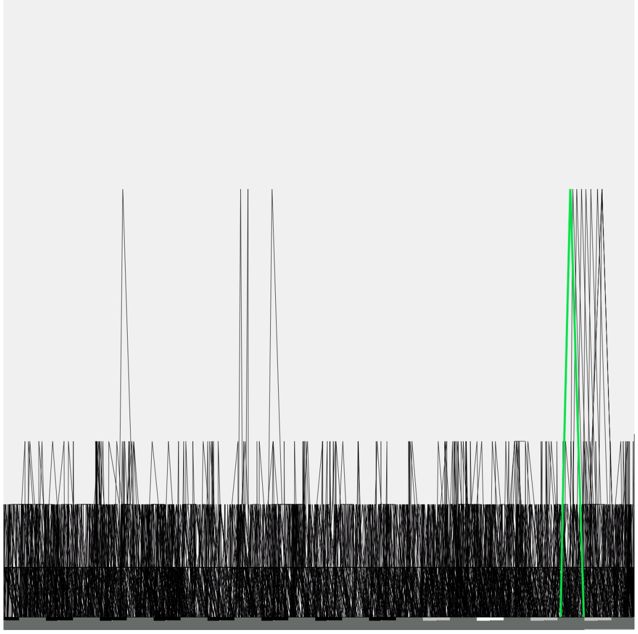

Figure 4: Line-based histogram representation of intrusion data. Time is shown on the X-axis and threat level (severity) is shown on the y-axis.

With the visualization environment, this unusual behavior sticks out like a sore thumb. Additionally, we have the ability to quickly analyze this activity to determine the meaning behind the user's behavior. In this scenario, what is actually occurring is that we have an academic environment in which an individual attempted to login to one of the public access computers multiple times. In fact, the individual attempted to log into one machine three times in a row (the standard time out parameter). The severity level indicated the failure of these attempts. The individual then attempted to log in to a second workstation, within the same lab, three times. A final attempt was made to login to a third workstation a single time. At this point the individual appears to have given up. Clearly, knowing this is an academic environment; it is obvious we have a student that has forgotten their password. This can be removed from consideration as a serious threat. The key, however, is the rapidity and detail to which the user's behavior can be analyzed. This is a critical ability for the intrusion detection community. Additionally, this example shows how the behavior and meaning of the behavior is critically dependent on the environment in which it occurs.

6.2 Static 2D Glyph-Based Visualizations

Figures 5 and 6 provide representations of the 2D glyph-based techniques. Figure 5 shows the host-based mode and figure 6 shows the user-based mode.

Figure 5 shows anomalies that do not stand out in any of the other examples. What we are particularly interested in are changes in activity. Some systems have continuous activity of high or moderate severity. Assuming this is not new for such systems then the activity is not of concern. Changes in behavior are clearly visible in some of the elements. It is these changes in behavior that are truly of interest. For example, one host one-third from the bottom stands out as it has many events initially at a high severity level before tapering off. Selecting these elements and examining the types of events indicates they are system events. It turns out the system had just been rebooted.

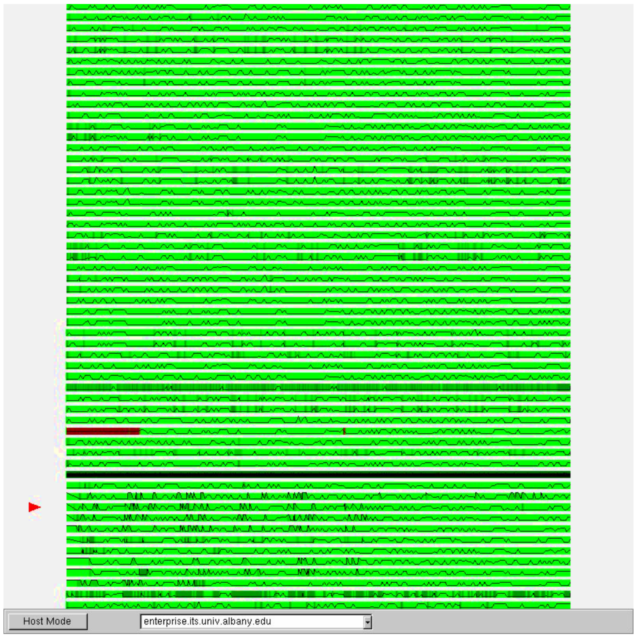

Figure 5: 2D glyph-based representation. Threat level (severity) is shown on a green → red scale. Time is on the X-axis and individual hosts are shown on the Y-axis. Connection information is represented through the histogram overlaid onto the color scale.

Figure 6 shows the expected behavior of users, applying the user-based mode, in that many fewer events are shown, particularly severe events, and each individual is connected to the system for varying lengths of time. Users with more frequent and more threatening activity could then be examined.

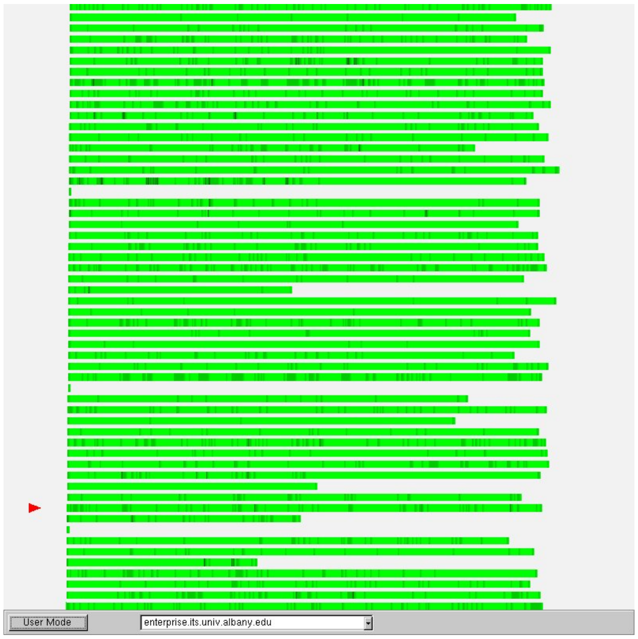

Figure 6: 2D glyph-based representation. In this scenario we are representing a per user model.

The line-based histograms provided in conjunction with these 2D glyphs are of particular interest and can identify unusual activity that otherwise would go unnoticed. For example, a single user who has suddenly changed their behavior and connected from a remote system when their history shows they generally connect from the same local host will be clearly shown through an isolated spike.

Additionally, a remote user with two connections ongoing simultaneously from different hosts will be distinguishable due to parallel lines, clearly a compromise or abuse of the account. Thus, in the user mode we can show not only relationships with the local connection information but also remote connection information.

Both these scenarios relate behavior indicated by system administrators as being critical to identifying compromised accounts. Previously, no techniques were readily available for easily identifying and analyzing such behavior.

6.3 Animated Glyph-Based Visualizations

The animated visualization techniques are designed to show a snapshot of system activity at any point in time. By animating the visualization, the analyst can watch activity over a specified period of time across the network as a whole. Given that most activity is instantaneous in nature, we provide a fade effect for all events. This is similar to the persistence provided by radar displays. Thus, elements remain on the display for some time after the event has completed to allow it to be perceived. The fade effect itself not only shows the event but also shows the fact that it has completed and will shortly be removed from the screen.

Examples of the animated visualization techniques are presented in figures 7 and 8. Figure 7 shows an example in which multiple remote connections fail in rapid succession. These are shown in red near the center of the screen. The remoteness of the system is indicated by the ring in which the node appears. Thus, these failed connections are essentially local systems. This type of behavior is indicative of someone attempting to identify characteristics of the system to attack. The fade effect is critical for showing the sequence of events.

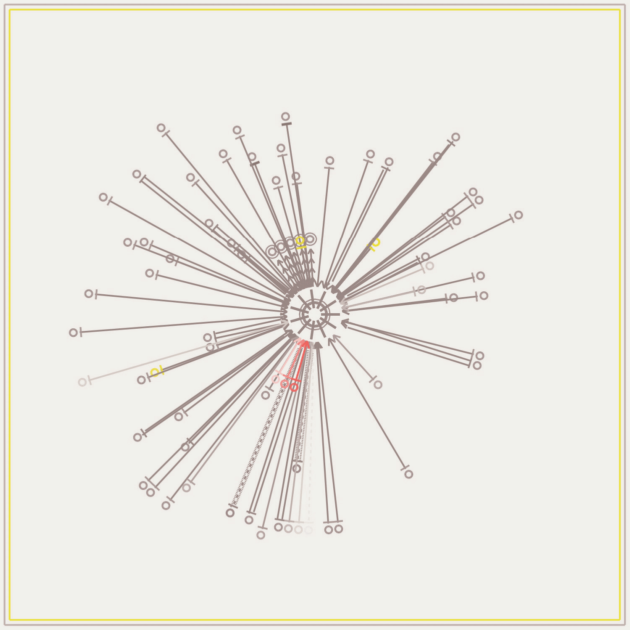

Figure 7: Example of a 3D glyph-based visualization with a single host. In this example, multiple anomalous activities in rapid succession are shown in red.

Figure 8 shows an example in which a user has connected through one system to reach another. More specifically, a remote user has connected directly to a local workstation. The individual then connects to the organization's server. The behavior stands out clearly due to the perceptual effects generated by the visualization techniques. More specifically, the node layout creates a characteristic 'V' shape in conjunction with many crossed lines. The analysis process is aided by probing, which identifies the user, verifies it is the *same* user, and identifies the hostname and IP address of the remote system (if available).

Additionally, a single local workstation is shown to be maintaining connections to many other systems. This is easily identified as being the system administrator but is anomalous behavior that should be analyzed and verified to be in fact what is expected.

Finally, the image shows many failed authentications (parallel lines shown in red). This is common in a university setting but also shows behavior seen in most organizations as individuals attempt brute force attacks on systems network-wide. The clarity with which this behavior stands out is critical for identifying potential attacks, especially should a system with such failed authentications be identified in conjunction with additional anomalous behavior at other points in time.

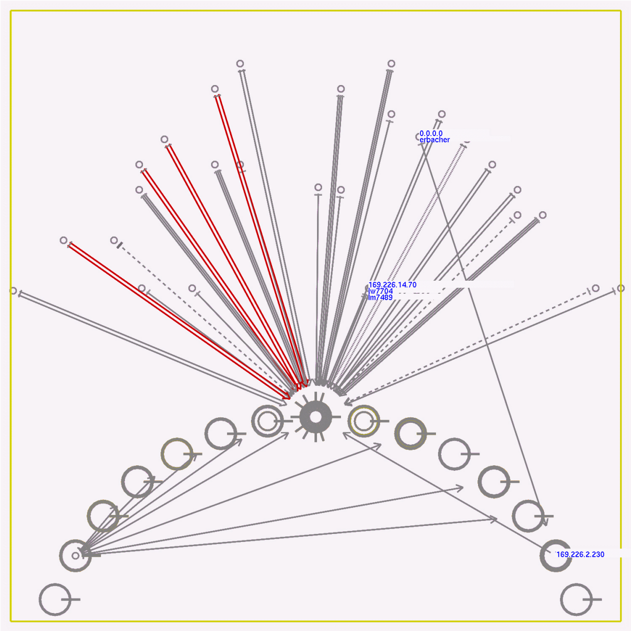

Figure 8: An example of a 3D glyph-based visualization . This example shows anomlous activity as a user connects *through* one system to get to another system, a single user with many local connections, and many failed authentications. These are common behaviors of an intruder.

7 Conclusions

In this paper, we have discussed the aspects of behavior critical to intrusion detection and monitoring as well as forensic analysis. We have further identified the aspects of behavior to be identified at multiple levels, including: user behavior, program/application behavior, and system behavior. Each of these areas must be completely examined and analyzed in order to fully meet the needs of intrusion detection and monitoring.

Given the volume of data that must be analyzed we have developed visualization techniques to assist in the monitoring and analysis processes. Behavior is critical to the success of this process and, consequently, the developed techniques were designed with understanding behavior in mind. The provided examples show the effectiveness of these techniques and their application to understanding and monitoring behavior.

Of particular interest is the ability to detect new behavioral patterns among intruders. We identified example types of anomalous behavior. Similar types of behavior should be considered questionable. However, most anomalous activity will be unique to an organization due to the network and security policies in place, the security protocols applied, the type of employees and users supported, the type of data maintained, and the advent of new techniques by attackers. As an analyst identifies novel attacks within their organization they will be able to easily categorize similar types of behavior.

8 Future work

The techniques we have applied are currently limited to system log files and statistics. While much can be gleaned from this information there remain weaknesses, primarily of which is the susceptibility of system log files themselves to attack. We are currently working to integrate network traffic data as well as kernel data. The incorporation of such results will greatly enhance the systems capabilities.

Additionally, we are continuing to explore new visualization techniques that can more effectively represent the diversity and volume of data available yet remains easily interpretable by system administrators.

Finally, we must provide additional examples of how the techniques are applicable to both common and previously unseen types of attacks and behavioral anomalies. The techniques show many forms of behavior and it remains to be seen if they can identify all anomalous behavior. This must be done in conjunction with more extensive categorizations of behavior for analysts to begin with before they begin identifying their own anomalies.

References

[1] Rebecca Gurley Bace, *Intrusion Detection*, Macmillan Technical Publishing, 2000.

[2] Richard A. Clarke, “Convergence and Transition, Privacy and Security,” Remarks at SafeNet 2000, Redmond, WA, December 2000.

[3] Robert F. Erbacher and Georges G. Grinstein, “Issues in the Development of 3D Icons,” *Visualization in Scientific Computing*, Springer-Verlag, 1995, pp. 109-123.

[4] Robert F. Erbacher, Z. Teng, and S. Pandit, “Multi-Node Monitoring and Intrusion Detection,” *Proceedings of the IASTED International Conference On Visualization, Imaging, and Image Processing*, Malaga, Spain, September 9 - 12, 2002, pp. 720-725.

[5] Robert F. Erbacher, Kenneth L. Walker, and Deborah A. Frincke, “Intrusion and Misuse Detection in Large-Scale Systems,” Computer Graphics and Applications, Vol. 22, No. 1, January/February 2002, pp. 38-48.

[6] Greg Farrell, “Police have few weapons against cyber-criminals. Problem stems from lack of funds, training,” *USA Today*, pp. 5B, December 6, 2000.

[7] Kevin Mandia and Chris Prosise, *Incident Response: Investigation Computer Crime*, Osborne/McGraw-Hill, 2001.

[8] http://www.snort.org