Visualization of Complex Attacks and State of Attacked Network

Anatoly Yelizarov*
Department of Computational Mathematics and Cybernetics, Moscow State University

Dennis Gamayunov†
Department of Computational Mathematics and Cybernetics, Moscow State University

ABSTRACT
This paper deals with the visualization of complex attacks. "Complex attacks" is used here to denote the type of attack which consists of a sequence of related events, namely a multi-step, DDoS attack and alike. While there are numerous systems to visualize events that occur in the network, most of them are too complex to perceive, and require several visualization modes. This work presents a technique whereby the operator, using visualization alone, is able to display the full picture of events occurring in the network. The main feature of this method is the high recognition ratio of complex attacks as the sequence of constituent common events.

Keywords: network security, visualization, complex attacks.

Index Terms: C.2.0 [Computer-Communication Networks]: General — Security and Protection; C.2.3 [Computer-Communication Networks]: Network Operations – Network Monitoring; H.5.2 [Information Systems]: Information Interfaces and Presentation — User Interfaces

1 INTRODUCTION

Complex attacks differ from simple ones in that the latter are events wholly unrelated to each other. While a simple attack is an action of the single violator aimed to exploit the single vulnerability, a complex attack is the purposeful pre-planned set of simple attacks or events.

Complex attacks present a great menace as they are used precisely because a majority of the attacks most significant to the violator represent a combination of some actions (simple attacks) aimed to achieve some of his/her goals.

The classic example of complex attack is DDoS (distributed denial of service), whose goal is to prevent the functioning of the target service. This goal is attained by means of a great number of simple actions, such as TCP connection requests (like in the case of TCP SYN flood).

The simplest solution to the attack visualization problem includes the use of an event journal in which every event is allocated a string keeping up information about it. The administrator later reviews the log file to figure out what was going on in his network. All interesting information (for example, the address the threat came from) he can find just by looking at relevant fields in the file. That method can solve the problem of visualizing one-step simple attacks; however in the case of complex attacks a simple journal log will be insufficient simply because the events within one complex attack are interrelated and the interrelations need to be recognized and displayed to the administrator.

* e-mail: tolya@lvk.cs.msu.su
† e-mail: gamajun@lvk.cs.msu.su

Difficulties with visualizing complex attacks arise exactly from the factors germane to their very nature, such as duration over time, decentralization and complex structure of interrelations within one complex attack.

This paper aims at creating a visualization mode that will allow the operator who is monitoring the network to rely on the screen alone, without performing any active operations other than monitoring proper, to perceive information both about ongoing simple events, and complex attacks in whole, with all their internal relationships. In so doing, the main requirement to that visualization scheme is to make possible visual estimation by the operator of such characteristics of the complex attack as:

- severity level;
- large-scale involvement;
- duration;
- relations to other attacks.

Our work is fulfilled within the existing project to produce a system of complex protection of corporate intelligence systems and networks from external and internal threats to informational safety. Accordingly, we will consider that all preprocessing of messages on network and local events has already been done by the intrusion detection system (hereinafter IDS).

The developed visualization scheme is presented in the third and fourth parts of this paper. The following part is devoted both to visualization systems and techniques in general, as well related works in the field of attack visualization, in particular. The fifth part will shed light on future work plans, and the conclusion will be found in the sixth part.

2 BACKGROUND AND RELATED WORK

2.1 Visualization Subsystem

The visualization subsystem is the IDS/IPS part responsible primarily to represent its work results in a system administrator friendly format. In other words, the visualization subsystem, due to some sort of abstraction, simplifies understanding of IDS output information for the human administrator.

The hardest part was associated with choosing the right abstraction. First and foremost, it should be amenable to direct perception by a human being (we will examine only visual perception): for this end, it must be made up of comprehensible visual images. The abstraction must likewise be informative and provide a maximum of useful information for the administrator while also maintaining its perceptibility. This requirement, as well as the specific character of the incoming information, makes it necessary to adjust this abstraction to the requirements of a given application.

Besides, in analyzing the abstraction for informative content, one must bear in mind the limited perception ability of the operator who should therefore receive, ideally, nothing but the information absolutely vital to his work. In parallel, he needs a capability allowing him to imagine the full picture of ongoing events in the network assigned to him. One example is the background IDS messages corresponding to random external attacks

by worms and viruses which are likely to result in the loss of information on an important purposeful act by skilled attackers.

2.2 Visualization Techniques

Basic to every abstraction is a certain procedure including a set of data mapping methods. Some systems employ various combinations of visualization techniques. Each methodology relies on its own unique way of data representation. For efficacy, any such methodology depends in large measure on the specific purpose it is designed to serve or the exact data type it helps display.

Clearly, no one visualization technique has the capacity to convey with an adequate degree of perception all characteristics required for the administrator. We have reviewed existing visualization techniques from the standpoint of their ability to help resolve our problem, and defined for any one technique the matching set of parameters best-served by it. Examples are:

- Histograms for any activity seeking instant comparison.
- Glyphs for mapping hosts and events, and glyph sizes for some additional information
- Scatter plot do well for local and external host relationships.
- Color maps show severity levels or attack type.
- Parallel coordinate axes have similar application patterns with scatter plots, with the only difference of having their respective parameters are aligned on the axes, rather than distributed in space.

We ended up with an abstraction based on a combination of these visualization techniques.

2.3 Related Work

To be sure, a "perfect" visualization system is non-existent, due to nothing else than the subjective nature of the perception process; as a result, no ready-made solution in this area can claim applicability for all cases. Of the great many visualization systems currently available, each meets well in its own effective way the objective it was designed to fulfill (whether event mapping in a small private network or conversely in a huge provider network).

None of the available visualization tools supplies in full the challenge of mapping complex attacks, in most cases for two reasons: because it is impossible to display the interrelations of events (to explain it, let us note that mapped information does not pass through the correlation system); and because information about time is not represented with sufficient clarity (e.g. for lack of a time axis).

Our work presents a different tool than others visualization techniques available in the area of information security precisely because it was originally designed with a focus on the visualization of complex attacks. Although the task seems specific, there have been numerous previous efforts in such closely allied areas as the visualization of attack or of event log:

- RADAR [4] / The Spinning Cube of Potential Doom [6] / gCube [7]. All these tools have at their basis a similar visualization procedure. Each event, whether completed or attempted connection, manifests itself as a color dot in the 3D cube, where the X and Z axes show local and external hosts, while the target host's port number is plotted over Y axis. An understanding of this situation comes about by means of visual recognition of such patterns as a line or rectangle. For example, port-scans are displayed by straight lines, parallel to the Y axis.
- VISUAL [5] – this tool allows users to see interaction of their internal networks with external sources. Visualization operates mainly by the method of scatterplot diagram. In this system the internal network is represented by a grid in which every cell corresponds to a local host. Each external host may be depicted by a square-glyph whose size matches the volume of packets transferred in the course of the host/internal network interaction. The interaction itself is plotted by a line extending from the source to the target. VISUAL can effectively present information on the networks with less than 2,500 internal nodes.
- Tudumi [8] is a 3D log visualization system aimed at displaying user activity. This is achieved by recourse to the scatterplot diagram having glyphs located on rings, consistent with the network nodes. Their shape represents the parameter of host type: whether user or external host. The color map technique is also involved in this system, its goal to distinguish among users; in Tudumi, each user can be assigned not only a telltale color but also a certain texture.
- RainStorm [2] is a tool for visualizing IDS alarms in a fairly large network (it was successfully tested on an exemplary network of 30,000 nodes). Any administrator who applies this tool is capable of recognizing the event's severity level, target host address and time of occurrence. Local hosts are plotted over multiple Y axes, using the parallel coordinate plot technique; time is shown on the X axis. Unlike the systems listed above, RainStorm does have an axis responsible for time, which makes time patterns recognizable. The severity level of a threat is portrayed with reliance on the standard application of color map technique: red, yellow, and green dots point to high, medium, and low concerns, respectively. Those pixels are plotted in a way consistent with the time and address of the target host. Functions e.g. scaling and filtering are applied in RainStorm to address the problem of information overlaps.
- Visual Firewall [3] visualizes firewall operations, IDS alarms and overall network security status through the use of four visualization modes. The mode Statistics illustrates the network's summary throughput capacity over time, relying on histogram color maps to identify the direction: purple for summary, red for incoming, and green for the outgoing throughputs. Other two views, Real-Time Traffic and Visual Signature, utilize parallel coordinate axes to plot the incoming and outgoing packets and flows as animated glyphs and lines respectively. Perception of the time taken by this activity is achieved by gradual glyph fading. The last visualization mode, IDS Alert, is implemented in a quad-axis space: the lower axis displays time, the left lists the IDS set of rules, and the remaining two represent local and external hosts. Every alert is mapped by a dot in the time and alert data 2D space, and lines trace the connection of a message about an event with the proper source and target hosts. Severity of that alert is indicated by an interplay of colors in the standard red-yellow-green menu.

The tools we have just examined add up to a wide range of visualization techniques that have been used here. Many of them are implemented to varying degree in our work and all have left numerous impacts on the visualization system we have developed.

3 Technical Approach

3.1 Choosing Priorities

Following Schneiderman's Visual Information Seeking Mantra ("Overview first, zoom and filter, then details-on-demand."), the tool being developed functions in two modes: main, providing information about priority parameters, and auxiliary, offering data of secondary importance to the task at hand.

One of the problems faced at the development stage included discrimination between the priority and secondary parameters just mentioned. This exercise proceeded by reviewing typical examples of complex attacks and simulating the subsequent situation on that basis.

Initial data. The network that we monitored consisted of twenty five hosts subjected at once to several attacks within a short time (10 seconds).

Distributed scanning. One attack amounted to distributed scanning of the network hosts. The key idea was that the attacker, in order to lull suspicions, relies for the source not on one host, but on the entire network under his control. As a result, targets and sources were engaged en masse for the attack, making its visualization so much more complex.

Multistep attack. Another attack had a multistep nature involving distributed scanning, node capture, remote acquisition of the administrator's root privileges at one of local hosts and a denial-of-service attack from it on another local host. The specific feature of this attack consists in its having, again, multiple target and source hosts and proceeding in steps, which in turn have different matching IDS messages both by type and severity level.

DDoS. Other attacks fall into the distributed denial-of-service category where the target host is exposed to multiple requests from various source hosts. This results in depletion of the target host's resources. Although this attack involves one target host, the amount of incoming messages over a short time is so huge that to perceive any information about other simultaneous attacks becomes an uphill task.

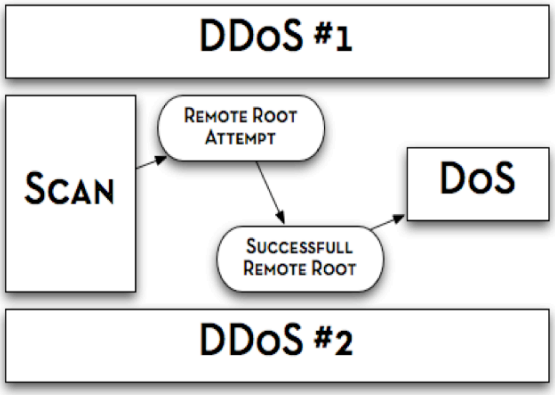

Fig. 1. Schematic representation of simulated situations.

In this simulated exercise, the administrator receives a great number of messages from IDS (about 200) in a very short period of time. The events he will see occurring differ in their type and level of severity. But because the attacks tend to intersect in time, the messages related to different attacks would occur intermittently. These factors unduly complicate perception by the administrator of the whole picture of developments in the network. He needs to understand clearly how many attacks (not events) have targeted his network, how long they will last, whom they are targeting and how severe they may be.

In order to identify priority parameters, work was done to simulate the administrator's required perception of the information to be provided by the system so designed.

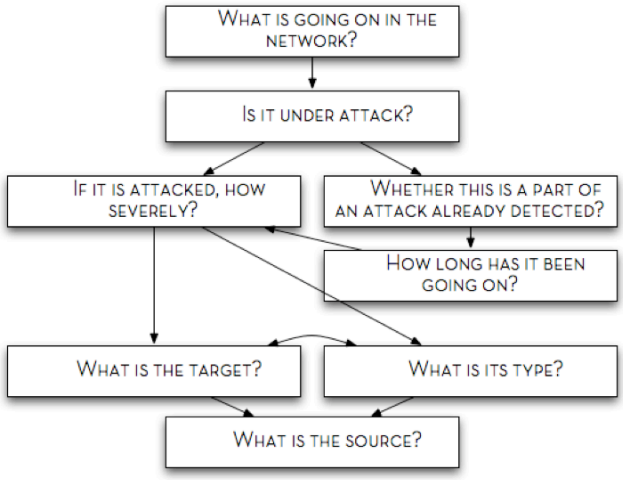

Fig. 2. A model of desired information perception by the administrator using the designed system.

In conclusion, severity level, target address, numeric strength/duration and interrelations with other attacks were recognized as priority parameters; type and source address were rated as secondary parameters.

3.2 Visualizing main properties of a complex attack

3.2.1 Level of Severity vs. Type of Attack

As an opening statement, our system should as far as possible display each network event (the only exception is made for the concurrent events targeting the same host; a more detailed treatment will be given below). Every one of these events has a matching glyph. For the glyph, we have chosen a cylinder which seemed a simple and clearly perceptible form to us.

Although each IDS sets its own severity levels, their range is mainly limited to three or four, as in the case of our project which provided a framework for our study. Its severity levels fall into low, medium, high and a special level of information messages.

For such a short range of values it is not feasible to allocate an entire axis. On the other hand, the severity level is an important parameter which calls for ease and accuracy of visual perception. Suitable visualization techniques can be found in color maps and glyph sizes.

The type of attack parameter is similar to the severity level in its short range of values (e. g. by comparison with possible network dimensions), but differs from it in that the type of attack values hardly lend themselves to alignment in an orderly fashion. This rules out the glyph size method for use to represent the attack type. Color maps, however, seem applicable as before, except that in this situation ambiguous recovery of the value is distinctly possible with more than six to eight different types (depending on the individual ability to distinguish different colors). Another solution to the problem includes texturing, with each specific type of attack matched by a certain texture.

Equally possible is an option with three axes where the glyph pointing to the attack will be identified as to its location by the time, target address and type of the attack. Yet in this case, too, unambiguous understanding of the displayed information is going to be difficult, due to complexities at the level of perception caused by the inevitable projection of a separate point onto the axes, as well as the overlapping glyphs.

As a result we opted for the one- dimensional representation of the glyph size (height of the cylinder) to recognize the severity level and for the color map to display the type of attack.

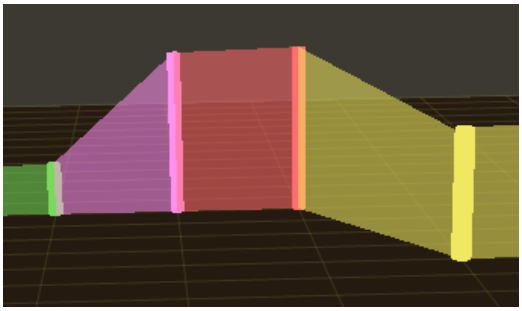

Fig. 3. Displaying a part of multistep attack with our newly developed system.

An example of visualizing four events from the multistep attack is provided in Figure 3. Each event is represented by a cylinder specific to it. Of these the low green cylinder suggests scan alert, in line with the choice of green color to denote scan type events; the severity level of that alert in our IDS is low so the cylinder height is low, too. Our further choices included purple to designate remote root attempt alerts and red to do so for successful remote root messages. These two IDS alert types present the highest severity level. The yellow cylinder matches the DoS type alert of medium severity.

As can be seen from the example in Fig. 3, our techniques of choice for representing the severity level and attack type make for the clear-cut perception of both these parameters.

3.2.2 Interrelations of Events within Attack

The key guideline in design of the system attempted to combine as one entity the events occurring in a complex attack. It was decided to realize this principle of visualization by successive linking of glyphs consistent with the events in the complex attack. In other words, every new event related to an already discovered attack is traced somehow to that attack's last event. This method enabled the administrator to perceive not only the relations of attacks within a complex attack but the latter's duration as well.

As can be seen from Figure 3, the relations of events within an attack correspond in our system to a quadrangle connecting the vertices of the associated cylinders. To reduce the likely information losses due to overlapping/screening, the linking elements were made transparent (default alpha-parameter is 0.5) to allow perception of both the events being screened and the very fact of linkage taking place.

It was likewise decided to introduce special visualization modes aiming specifically to represent the type of complex attacks in which glyphs pertaining to the attacks' events are displayed so as to prevent the intersection of their connecting elements. This solution guaranteed to the administrator better perception of complex attacks.

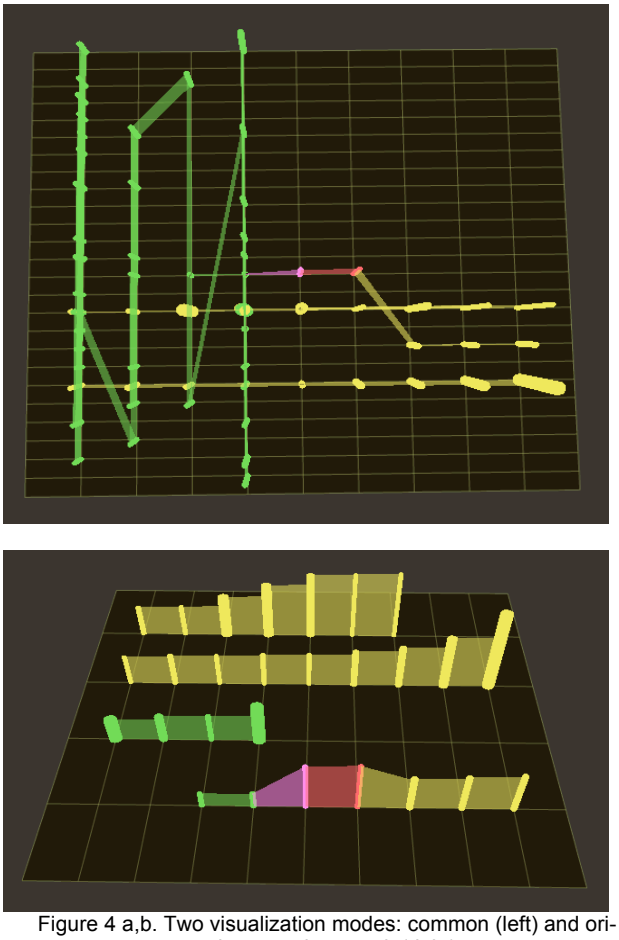

Figure 4 a,b. Two visualization modes: common (left) and oriented to complex attack (right).

Operation of the designed visualization system is demonstrated in Figure 4 using the example of distributed scanning (interlinked green cylinders) of the above-mentioned multistep attack and two DDoS'es (yellow cylinders aligned in a row). Altogether, either drawing in Figure 4 shows the situation following 200 alert messages in 10 seconds. In spite of so great an amount of displayed messages, the complete picture of what has occurred is easy to perceive, showing clearly the number of attacks involved the events involved in a particular attack.

3.2.3 Time and Visualization Space

As can be guessed from Figures 3 and 4, visualization in the designed system actually unfolds in a 3D space. This solution met with acceptance by virtue of giving more opportunities to portray a maximum number of parameters. An overview of the now available visualization tools shows that the best time perception is achieved with its linear mapping, by letting time have a corresponding axis.

There are three ways to allocate coordinates in a 3D space: classical (Cartesian), cylindrical and spherical (polar). The option with spherical coordinates offers a poor solution to the problem in hand, as the only axis will be setting time and thus creating difficulties of perception. This is because the different surface areas consistent with different time lengths will bring about inevitable overlap and data losses. Both remaining options (Cartesian and cylindrical) are implemented in our system, as is the opportunity of mode-to-mode switching.

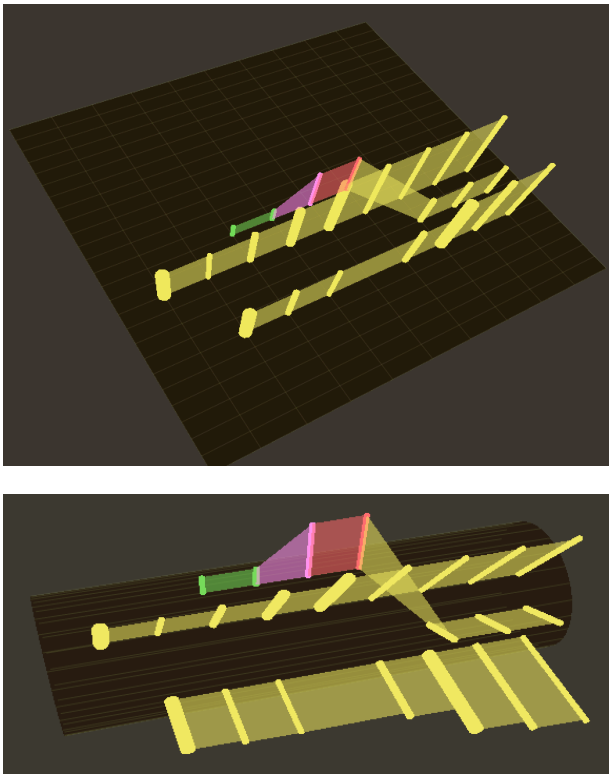

Figure 5 (a,b). Designed system's operation in two space allocating modes: Cartesian (left) and cylindrical (right), as exemplified by multistep attack and two DDoS'es.

While the Cartesian option is more common for perception, the cylindrical space allocation has the advantage of providing a larger volume of space between two neighboring glyphs. That can be seen at Figure 5b as a consequence of the angle between cylindrical glyphs departing from naught (in the Cartesian space, the corresponding cylinders run parallel). This contributes to greater accuracy and precision in perceiving the information which is represented between those glyphs; this latter case refers to the last part of a multistep attack which is itself the DoS targeting the node displayed just between the nodes which were subjected to DDoS-attacks.

3.2.4 Hosts' addresses

It was decided to put one of the axes in the case of Cartesian space, and the angle in the case of cylindrical coordinates in correspondence to the address of an attacked host in the internal network. The conceptual difference of mapping between the target and source addresses is that, to the administrator, all external hosts are equivalent in terms of hazard each of them is likely to hold out. Rather than the address of the source of an attack (which is definitely significant information which the designed system ought to represent), he needs to know how many sources set off a concrete attack and whether a given external host is itself the source of several detected attacks.

Conscious of these properties of external hosts, we decided to map them with either a scatterplot diagram or parallel coordinate axis. To do so, a subsidiary axis was added for plotting the external hosts' addresses, wholly unrelated to the previously introduced visualization space. When one, several or even a series of events was to be selected, the sources generating them were connected by straight lines to the glyph of a compatible target. The straight line was given a color matching the type of the appropriate event, which made it possible to see not only how many times a particular host sourced a hazard, but also the types of hazards provoked by it.

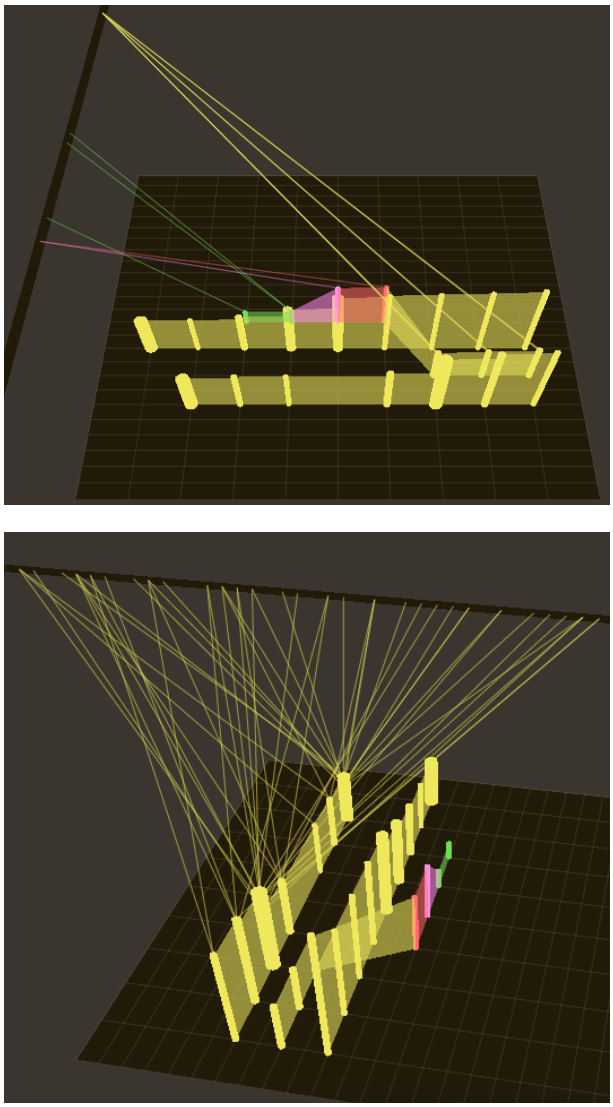

Figure 6 (a,b). Designed system's tool for displaying external hosts.

All sources of the multistep attack referred-to above are represented in Figure 6a. Thus one can clearly see, for example, the host chiefly provoking the attack and performing the “remote root attempt” and “remote root” events. Figure 6b represents the situation in displaying sources of one specific DDoS. As the result of this visualization there arises a clear view of the attacker's botnet as well as the distributed nature of the attack.

For the source axis, the following set of actions is proposed: the twofold opportunity to hide it if not needed or if the perception of the remaining picture is prohibitively complex. Or, conversely, to reveal it or move to a convenient spot for the administrator.

Due to the difficulty of perceiving an exact address from a dot on the axis, the precise values of target and source host addresses, as well as the exact time also preset by the axis, were thought to be best displayed in the auxiliary mode, with the cursor position above the event of current interest.

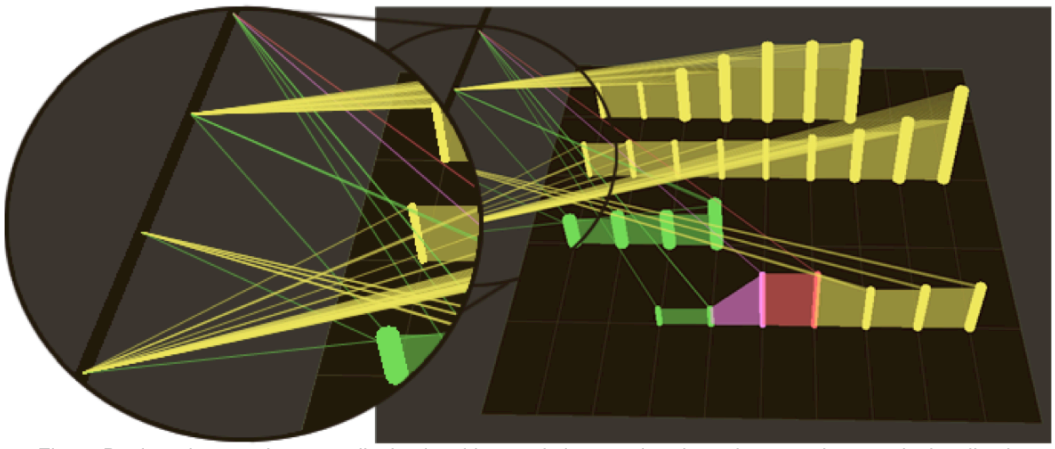

Fig. 7. Designed system's use to display local host axis in a mode oriented to complex attack visualization.

As stated above, additional modes were introduced to improve perception of complex attacks, oriented to displaying these attacks. The modes stood apart for assigning priority, not to the address of an attacked host, but instead to the property of connection among events within a complex attack. On the very axis where local hosts' addresses were plotted in the common mode, each point corresponded to a certain complex attack in the special mode. As a result, there arose a complex structure of connections among various attacks, which do not intersect. The underside however was the loss of information about the target address.

Seeking to display this information, we introduced again a new axis divorced from the main visualization space, to plot local host addresses. Thus, in the mode oriented to displaying complex attack in Figure 7 one can clearly see all four attacks listed above, but at the same time is able to perceive information about what host was hit by what attack.

3.2.5 Other functional features

Due to various limitations, information regarding the time of an event can only be given accurate to one second. In this day and age when a multitude of events occur in one second, it is highly probable for several events to happen to one host at the same time. To portray such a situation, we opted for increased glyph thickness, in line with the quantity of the events to be represented at that point in the visualization space. There is a limit however imposed on the maximum glyph thickness with a view to avoiding overlap/intersection of neighboring glyphs.

Fig.7. Glyph thickness and height variations with frequency of events.

The system we designed can map the parameter of frequency at which events tend to occur. If events in the network are interrelated and their frequency exceeds a certain threshold (which the system administrator is free to set independently) the appropriate glyph length will be increased. This feature, in other words, sends up the severity level of events according to their frequency, rendering them more noticeable to the administrator.

The increasing glyph height proceeds geometrically, i.e. the more frequent an events, the faster the glyph height increase and the better its visual perception. Each frequency threshold is matched by a certain coefficient (it is only prudent to match a greater coefficient with a smaller time interval).

Figure 7 shows a part of the DDoS attack. In principle all events within an attack are of the same type and severity level. But because the glyph height increases with the frequency of events (and the DDoS-attack is bound to entail an excess of the frequency threshold) that attack becomes appreciably more noticeable for the administrator.

3.3 Closer Look at Visualization Modes

The designed module was earlier said to offer the user four different visualization modes. They all share the event glyph shape - the cylinder, whose height corresponds to the severity level and frequency of that event. The glyph's various colors point to different attack types. Also, in every mode one has the option to recall auxiliary axes of internal/external hosts. Below we will look closer at every visualization mode, with an accent on the dedicated use of each one.

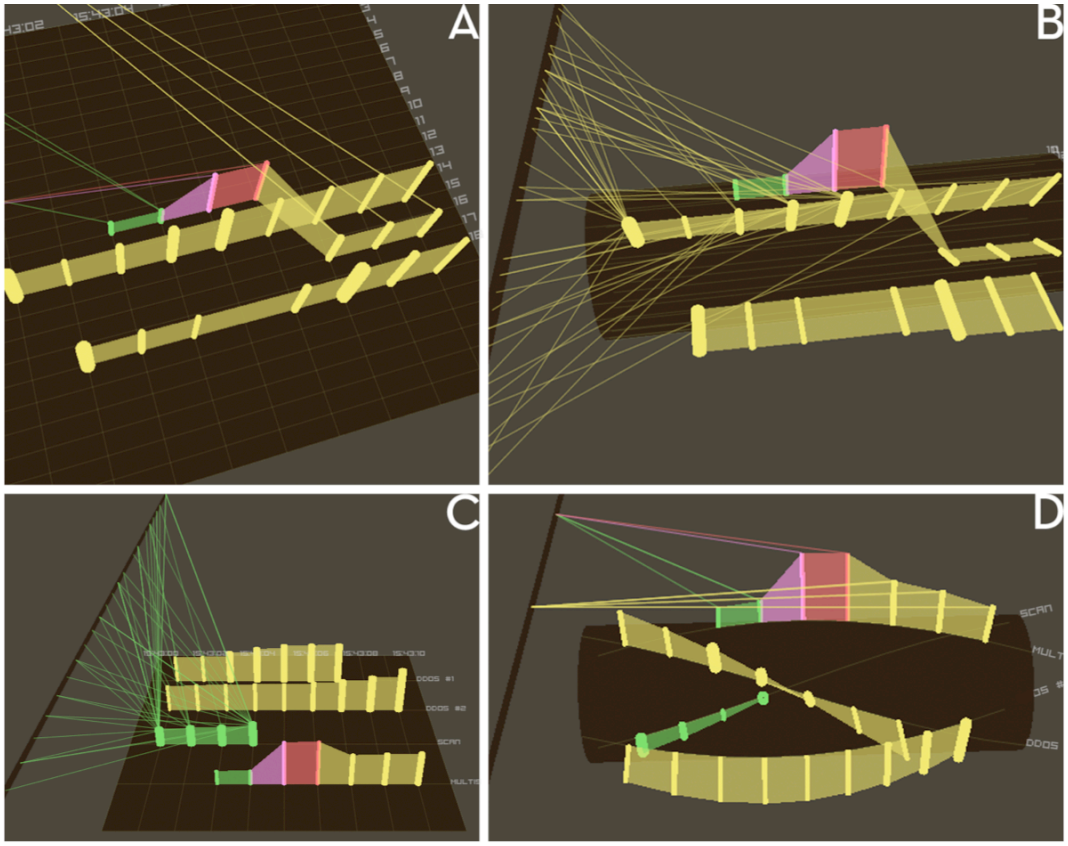

Fig. 8 (a,b,c,d). All four visualization modes as exemplified by distributed scanning, multistep attack and two DDoS'es. Every attack consists of about 50 events.

3.3.1 Planar common

This mode presents itself as a visualization space in the classical Cartesian coordinates, where internal hosts are measured over the left axis and time is shown left to right (a more recent moment in time appears on the right). The location of every glyph is uniquely defined by its time of occurrence and the target host address.

The key application feature of this mode converges on clear-cut perception of "topology" of the attack; indeed it is clearly seen in Figure 8 that first came scanning and capture of host #13, followed by the DoS type attack on host #17. At the same time, hosts # 15 and 19 were subjected to DDoS-attacks.

3.3.2 Cylindrical common

This visualization mode maps all information on the same principle as was described above for the common planar mode, except that the visualization space is allocated by cylindrical coordinates. As a consequence, internal hosts are preset by the angle rather than axis.

The cylindrical mode was introduced for its ability to provide better opportunities for perception by comparison with the planar option. In the cylindrical view, the space between neighboring glyphs is greater, so the information losses due to overlap are lower than in the planar case. Thus more accurately perceived in Figure 8b are developments in the host range of nos. 16 to 18, which in the planar case was obscured by the DDoS'es "membranes".

3.3.3 Planar, oriented to complex attacks

Whereas our whole set of tools is designed to visualize complex attacks, the following two modes sought to enhance better perception of each attack at the sacrifice of a fraction of information regarding attack objectives.

The horizontal axis, as before, is the time axis, and every coordinate on the vertical axis corresponds to a certain complex attack. The axis scaling varies with the emergence of new attacks (but not new events in the attacks detected thus far).

The mode's distinguishing trait is that the length of a complex attack in the visualization space agrees with its duration - a feature absent from the previous two modes whose projection onto the time axis is not equal to the summary length of all "membranes", because of their extension non-parallel to the time axis.

This mode offers the most easy perception of both, the duration of complex attacks and their co-location in time (e.g. in Figure 8c it is seen how the multistep attack started right after distributed scanning). In other words, while the common modes feature better perception of the attack's "topology", the two special modes excel in the perception of its "chronology".

Inadequate perception of the target address information is presumably offset in some degree by the auxiliary local host axis whose functioning was described above. In Figure 8c one can clearly see the large-scale involvement of distributed scanning which affected almost all the observed network.

3.3.4 Cylindrical, oriented to complex attacks

The principle of visualization in the last mode is related to the above notion of improved perception of complex attacks but at a sacrifice in the information about internal hosts. The difference

lies with the uniqueness of cylindrical space allocation: a larger inter-glyph space diminishes the information losses due to overlapping glyphs.

For the more convenient real-time perception of ongoing network events, every attack is displayed, not along a straight line, as in the previous mode, but by a spiral, as if winding over time around the main cylinder, that is, the visualization surface. With this tool, the administrator can afford to observe inactively the given mode - not perform any actions with the visualization space and still end in the course of time up with the complete picture of ongoing events.

4 RESULTS

4.1 Inbuilt Module

As part of this work, a visualization module was developed on the basis of the previously described key visualization diagram. The module employs the OpenGL library and is implemented as an expansion of the administrator's console that controls the IDS being designed. In addition, the module visualizes the IDS-provided and pre-correlated data given below:

- time of occurrence of event;
- type of attack;
- severity level;
- reference to other events within the same attack;
- address of target and source hosts.

The inbuilt module realizes all these ideas regarding visualization of complex attacks:

- The four data presentation modes so implemented include: planar and cylindrical, which conform with the Cartesian and cylindrical systems of coordinates; and two special modes oriented to displaying complex attacks.
- Every event is identified by glyph-cylinder whose height indicates the severity level of a given attack and its color , the type of the attack.
- The glyph's location is identified by the time of occurrence of the related event as plotted on the time axis, and the source address positioning on the local host axis for instances of the planar mode and the angle for the cylindrical mode.
- Successive events within a complex attack are connected with a quadrangle having its vertices at the base and top of the appropriate glyph cylinders. The quadrangle is similar in color to the latest of the events it connects; also it is transparent in agreement with the alpha-parameter which is assigned to this color.
- Visualization is available for any time interval of interest to the administrator.
- If so desired, one can either reveal or hide the source host axis. The latter is realized in form of an extended cylinder located a little sidewise from the main visualization plane.
- Connections of events with external sources are presented in straight lines drawn from the requisite point on the source axis to the top of the related glyph cylinder. In color, the line corresponds to the type of the event with which it is connected.
- As well for the two modes oriented toward complex attack visualization, it is possible to display the internal host axis. Interconnections of the internal hosts and events are displayed by straight lines, following the principle described above for the links with external sources. Each straight line is color-consistent to the type of event it is connected with.
- The implemented system possesses an event frequency perception capability which responds with an increased glyph height and thickness whenever the frequency threshold is exceeded.

For more convenient use of the system, the user may access the following features in the inbuilt module:

- Rotation of the system of coordinates and the opportunity to view the situation at any angle for more integrated perception of the displayed situation. At the same time, when it was required to present the auxiliary axis of external sources in the cylindrical modes, we have opted for keeping it immobile while the cylinder rotated so as to better perceive the structure of ties between events and hosts.
- Scale variation has become also possible both on the time axis and more generally, all through the visualization space, allowing a more detailed view at the developments of current interest.

5 CONCLUSIONS

The tool we have developed is well-suited to display complex attacks. While operating capability the administrator is able to perceive important parameters of complex attacks, such as:

- duration over time;
- interrelations of events within one attack;
- severity level;
- types of component events;
- frequency of events in an attack;
- addresses of targets and sources.

Ready availability of several visualization modes offers the benefit of displaying the ongoing situation from different points of view. Coupled with the capacity for visualization space rotation, this provides an effective tool toward complete and integrated perception of the current status of events.

6 FUTURE WORK

In future, we intend to render our system more flexible. The triple objective is to let the administrator operating it select colors and textures for various attack types at his discretion; re-sort local hosts; and vary “on the fly” the types of parameters including height and frequency threshold of events.

Also plans are ahead to make the system user friendlier by offering the ability to perform standard and natural operations with the mouse e. g. selection of a rectangular area and dragging to tackle the tasks like selecting the events of interest and re-sorting hosts, respectively.

REFERENCES

[1] Rawiroj R. Kasemsri, A Survey, Taxonomy, and Analysis of Network Security Visualization Techniques, under the direction of Ying Zhu, Geordia State University, US, 2005.

[2] Kulsoom Abdullah, Chris Lee, Gregory Conti, John A. Copeland, John Stasko. IDS RainStorm: Visualizing IDS Alarms. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 1-10, 2005.

[3] Chris P. Lee, Jason Trost, Nicholas Gibbs, Raheem Beyah, John A. Copeland. Visual Firewall: Real-time Network Security Monitor. In IEEE Workshop on Visualization for Computer Security, 2005. (VizSEC 05), pp. 129-136, 2005.

[4] Hyogon Kim Inhye Kang Saewoong Bahk. Real-Time Visualization of Network Attacks on High-Speed Links. In IEEE Network, Volume 18, Issue 5, pp. 30–39, 2004.

[5] Robert Ball, Glenn A. Fink, Chris North. Home-centric Visualization of Network Traffic for Security Administration. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, ACM Press, Washington DC, USA, pp. 55-64, 2004.

[6] Stephen Lau. The Spinning Cube of Potential Doom. In Communications of the ACM, Volume 47 , Issue 6, pp. 25-26, 2004.

[7] Gregory Travis. GCube: Effective Network Visualization for High-Speed, High-Volume Networks. In SEI Conference, 2008.

[8] Tetsuji Takada, Hideki Koike: Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs. In Sixth International Conference on Information Visualisation, 2002. Proceedings, pp. 570-576, 2002.

[9] Daniel A. Keim, Florian Mansmann, Jorn Schneidewind, Tobias Schreck. Monitoring Network Traffic with Radial Traffic Analyzer. In 2006 IEEE Symposium On Visual Analytics Science And Technology, Baltimore, MD, pp. 123 - 128, 2006.

[10] Stefan Axelsson. Visualisation for Intrusion Detection: Hooking the Worm. In The proceedings of the 8th European Symposium on Research in Computer Security (ESORICS 2003), volume 2808 of LNCS, 2003.