Interactively Combining 2D and 3D Visualization for Network Traffic Monitoring [*]

Erwan Le Malécot
Institute of Systems & Information
Technologies/KYUSHU
2–1–22, Momochihama, Sawara-ku, Fukuoka
814–0001, Japan
lemalecot@isit.or.jp

Masayoshi Kohara
Graduate School of Information Science and
Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka
819–0395, Japan
kohara@itslab.csce.kyushu-u.ac.jp

Yoshiaki Hori
hori@csce.kyushu-u.ac.jp

Kouichi Sakurai
sakurai@csce.kyushu-u.ac.jp

Graduate School of Information Science and Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, 819–0395, Japan

ABSTRACT

With the multiplication of attacks against computer networks, system administrators need to monitor carefully the networks they manage. However, that monitoring task is made harder because of the increasing amount of data to process. Conventional automated tools provide limited support and most of the time require high skilled operators. Recently, tools using visualization techniques started to be proposed to resolve those issues. In this paper we introduce an original visualization design which combine 3D and 2D representations of the network traffic and activity. Both representations are based on the same interactive grid representation of the network space and are linked together as they provide complementary functionalities. The 3D representation provides an overview of the communications between several network zones and the 2D representation provides a detailed view of selected parts of the 3D one. A prototype was built according to the proposed visualization design.

Categories and Subject Descriptors

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

General Terms

Security

Keywords

Visualization, 2D, 3D, Network, Monitoring, Security

1. INTRODUCTION

Nowadays, many organizations heavily rely on computer networks which then become critical parts of their infrastructures. At the same time, the number of malicious attacks against such networks is exploding. In order to guarantee the security and the stability of the networks they manage, system administrators must monitor them efficiently. That monitoring task can be done displaying selected information about the network traffic in a textual form and reading this output directly. Unfortunately, the amount of data captured on the network they need to analyze to perform that task tends to become quite huge and that method is no longer really feasible. Various tools exist to help system administrators dealing with this issue. They are mainly based on automated systems (learning techniques, signature databases or statistical analysis).

Recently, visualization techniques also started to be used for the monitoring task. The idea is to take advantage of human visual processing and pattern recognition that are rather unexploited resources in traditional tools. Various visualization tools for network monitoring already exist. Most of these tools are built around 2D visualization zones. Some try to exploit 3D as it permits to create more complex representations, however they generally face clarity and usability issues.

In this paper, we introduce an original visualization design for network traffic monitoring which uses 3D. Network zones are represented by textured cubes. The textures of these cubes are modified according to the activity of the associated network zones. The network traffic is displayed as colored links between the cubes, the color standing for a chosen attribute of the traffic. As a 3D representation alone is most of the time difficult to manipulate and ana-

[*] Support for this work is partially provided by National Institute of Information Communications and Technology (NICT), Japan, as a visualization technology research for the *nicter* Incident Analysis Center project.

VizSEC'06, November 3, 2006, Alexandria, Virginia, USA.
Copyright 2006 ACM 1-59593-549-5/06/0011 ...$5.00.

lyze, we chose to combine it with an additional 2D representation. That 2D representation consists of two interactive grids standing for selected network zones. The activity of the hosts and the associated network traffic are displayed on that 2D representation too. The two visualization zones are linked together so that it is possible to synchronize some parts of the 3D representation with the 2D interactive grid system. To our knowledge, no other visualization tool for network traffic monitoring chose to combine 2D and 3D representations that way to enhance the clarity and usability of the full system. To evaluate our original approach, we implemented a prototype built according to the proposed visualization design.

This paper is organized as follows. In Section 2, we describe and analyze several existing visualization designs for network traffic monitoring and network security. In Section 3, we explain our original visualization design. In Section 4, we introduce the prototype we built following this visualization design and present some interesting patterns we were able to visualize with it. In Section 5, we conclude on the use of that prototype and finally in Section 6, we discuss some future work we plan to do in relation with the proposed visualization design.

2. RELATED WORK

The idea of applying visualization techniques to the field of network security and more especially to network traffic monitoring is quite recent. However, research has been active in the field of information visualization for a lot longer. Shneiderman proposes a taxonomy of information visualization techniques sorting them according to the type of data visualized but also according to the task to be accomplished [10]. It provides a large panel of available basic techniques that can be combined to make complex visualization systems. He also introduces the mantra: "Overview first, zoom and filter, then details-on-demand". We built our visualization design keeping that mantra in mind as we believe it provides a good list of required functionalities for an efficient visualization system.

Several tools already exist to monitor networks graphically. Most of them are based on 2D display zones. EtherApe [1] displays hosts as nodes laid out in a circle. Network activity is symbolized by the thickness of the links between the nodes and colors are used to represent the recognized protocols. This tool is well-suited to monitor a limited number of hosts. However, as the number of hosts increases, the visualization zone becomes difficult to interpret.

VISUAL [4] is another 2D visualization tool. It focuses on the display of the communications between the local network that the system administrator wants to monitor and the outside world. The monitored network is represented by a grid whose quadrilaterals each stand for a host. External hosts are represented as markers laid around the grid. Connections between internal and external hosts are symbolized by segments linking the markers and the associated quadrilaterals. The color of the segment indicates if the communication is bidirectional or unidirectional. The communication bandwidth is encoded in the size of the markers. VISUAL provides an efficient view of the interactions between the monitored network and the outside but the number of external hosts that can be represented is limited. Also, the internal activity of the monitored network is not displayed whereas a lot of network attacks come from the inside.

As for 3D visualization tools, the Spinning Cube of Potential Doom [6] displays data regarding established TCP connections and connection attempts on a cube. The x-axis of this cube stands for the local network's IP address space, the z-axis for the global IP address space and the y-axis for the TCP ports. Each TCP connection is displayed by a dot. This dot is white for an established connection and colored according to the port number for a connection attempt. In this way, connection attempts are emphasized and portscans are easy to detect as they appear as large colored zones on the display. However, after the detection, the exact origins of those attacks are difficult to retrieve using this tool.

IDtk [5] is another 3D visualization system. It can process either raw TCP network traffic or Intrusion Detection System (IDS) output (alerts). IDtk is based on the display of glyphs whose attributes are used to represent the components of the input data. These components can be encoded in the coordinates, the color, the size and the shape of the glyphs. With this tool, the user is free to customize the visualization zone. However, the design is limited as it only permits the detection of relationships between elements of the data, the interactions between the hosts are difficult to understand.

Oline and Reiners [9] propose several 3D visualization designs for network security using either raw network traffic (TCP and UDP) or IDS output. They were able to detect several anomalies with each visualization tools they implemented according to their designs. However, with some of their tools, it is difficult to get detailed information about the traffic displayed such as for instance the addresses of the hosts involved. Also, the interaction with the visualization zones of each tool is limited to modifications of the viewpoint in the 3D space using camera transformations.

3. THE VISUALIZATION DESIGN

The visualization design we propose in this paper derives from a 2D visualization design we previously introduced [7]. That previous design has some usability and scalability issues that we tried to solve exploiting 3D visualization techniques. So the objective of the current visualization design is the same as the previous one. We want to provide system administrators with both a view of the internal traffic of the networks they monitor and a view of the interactions of these networks with the outside world.

To this end, we chose to interactively combine two different representations of the network traffic, one in 2D and the other in 3D. Both of them are based on a grid representation of selected network zones. That grid representation is adapted to the IPv4 network address space. The information that we display on the resulting representation is to be extracted from IP network packets. It includes: the source IP address, the destination IP address, the source port, the destination port and the protocol. We are also displaying the time of capture of the IP packets.

3.1 The grid representation

The core component of our visualization design is a hierarchical representation of the network space based on interactive 16x16 and 256x256 grids (Fig. 1). Using this system, the user can access and visualize the activity of any network part, ranging from the global network to a single host.

The hierarchical representation is composed of five layers. The grids corresponding to the first four layers are 16x16

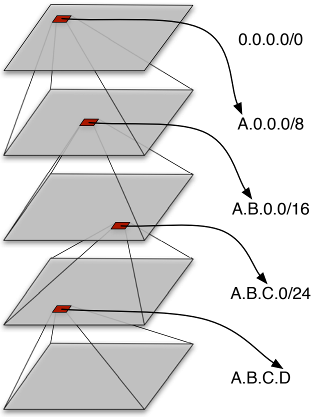


Figure 1: Interactive grid system.

and stand for network zones or hosts. Hosts are mapped on the grids according to their IP addresses. In the IPv4 system, IP addresses are coded by 32 bits which can be grouped in four bytes, as it is done for the dotted quad notation. In the initial state (layer one), hosts are mapped on the grids based on the first byte of their IP addresses. It means that a layer one grid stands for the 0.0.0.0/0 network zone and that each of its quadrilaterals is associated with all the hosts whose IP addresses share the same first byte. From this state, a quadrilateral can be selected and then, a layer two grid replaces the previous layer one grid. For instance, if the selected quadrilateral corresponds to the byte 192, the displayed layer two grid stands for the 192.0.0.0/8 network zone. Each quadrilateral of that new grid is associated with all the hosts whose IP address starts with the byte 192 and whose second byte is the value mapped on the quadrilateral. In the same way, a quadrilateral of that layer two grid can be selected, for instance 168, and in this case, the layer three grid standing for the network zone 192.168.0.0/16 is displayed. Finally, a third byte can be selected and at this point, each quadrilateral of the resulting layer four grid stand for a unique host. To represent the single hosts (layer five), we use 256x256 grids whose quadrilaterals stand for TCP/UDP ports.

To map the IP addresses bytes on the first four layers grids, we chose to use a quadtree scheme as it permits to gathers hosts in subnets on the grids and so to respect the network topology. For the layer five grids, we chose to use a coordinate system which was previously employed by McPherson et al. for their PortVis tool [8]. One axis corresponds to the port number modulo 256 and the other axis corresponds to the port number divided by 256.

3.2 The 2D representation

The 2D representation is composed of two interactive grids which behave as described in Section 3.1. One of the grids stands for the host(s) as source(s) (referred to as source grid from now on) and the other one for the host(s) as destination(s) (referred as destination grid from now on). The network traffic is displayed on that representation as lines joining the quadrilaterals standing for the associated source and destination zones or ports (for layer five grids). One line is drawn per packet captured and lines are colored according to the protocol of the packets. To represent network activity, the quadrilaterals of the grids are colored according to the number of packets sent, for the source grid, or received, for the destination grid, by the associated network zones. The higher the number of packets, the brighter the color.

3.3 The 3D representation

The 3D representation is based on textured cubes laid out in a 3D space. Each cube stands for a network zone (which can be either /0, /8, /16 or /24) or a single host. Faces of a cube are textured with grids (as described in Section 3.1) representing the network zone or the host the cube is standing for. Three faces of each cube are mapped with the associated source grid (referred to as source faces from now on) and the other three faces are mapped with the destination grid (referred to as destination faces from now on).

The activity of the network zone or host associated with a cube is represented the same way as for the grids of the 2D representation, encoded in the color of the quadrilateral of the grids mapped on the faces. Two different color scales are used in order to differentiate the source and destination faces.

A source face of a cube can be connected to a destination face of another cube. If so, the traffic from the network zone represented by the first cube to the one represented by the second cube is displayed between the two cubes. For each packet captured, a cone is drawn between the corresponding quadrilaterals on the connected source face and on the connected destination face. Using cones permits to display the direction of propagation of the packets. The time of capture of the packets is shown using a transparency effect. The older the packet, the more transparent the cone. In addition to that, the cones are colored using the same color scale as the one used for the lines of the 2D representation.

3.4 Interactions between the 2D and the 3D representations

The captured network traffic is displayed simultaneously on both 2D and 3D representations. The 3D representation provides an overview of the traffic between several selected network zones and hosts. The use of 3D brings flexibility as, for instance, if the user wants to monitor an additional network zone, he can add the corresponding cubes to the representation. Also, navigation in a 3D space is rather intuitive and users can easily modify the viewpoint to focus on parts showing suspicious behaviors. The 2D representation provides a view of the packets being exchanged between two selected network zones and the user can interact with the grid system to get more detailed information about that traffic. Compared to the 3D representation, the 2D one is more straightforward. Besides, interaction with objects is easier in the 2D space than in the 3D one. So the basic idea is to efficiently combine the two proposed representations as they provide complementary functionalities.

A pair of two cubes can be selected and the traffic between the two associated network zones is then displayed on the grid system of the 2D representation. Similarly, a pair of two cubes can be synchronized with the grids positions of the 2D representation so that the network zones represented by the grids also become the network zones represented by the cubes. It enables the user of the visualization system to analyze finely (using the 2D representation) suspicious network traffic that he detects on the overview (3D representation). He can use the grid system to "zoom" and select the involved network zones and hosts. If the suspicious network traffic happens to be malicious, the user can modify the settings of the overview to, for instance, add new cubes and synchronize them with the grid system. Doing so, he can keep an eye on that traffic and finely monitor it from the 3D representation. The user is able to create his customized cube layout to meet his own needs selecting the network zones he wants to monitor.

4. THE PROTOTYPE

4.1 Implementation

In order to test the accuracy of our approach and to be able to conduct usability studies, we wrote a prototype in C language based on the proposed visualization design. It uses the GTK+-2.X [2] library and GtkGLArea (OpenGL widget for GTK+-2.X) for the Graphic User Interface (GUI), and the Libpcap [3] library for the packet capture. It is known to compile and run on FreeBSD, GNU/Linux and Mac OS X operating systems.

4.2 User interface

The interface of the prototype is organized in four tabs:

- The "Visualization" tab: This is the main screen of the prototype. From this part, the user can visualize both the 2D (on the right side) and the 3D (on the left side) representations of the network traffic. On the center, the user can access several controls which are also grouped in several tabs:
  - The "Capture Controls" tab ("C"): It provides the controls to start a live packet capture and to open a previously saved network traffic dump file.
  - The "Visualization Controls" tab ("V"): It provides controls regarding the visualization zones.
  - The "Grid & Cube Controls" tab ("G", Fig. 4): It provides controls to select cubes and pairs of connected cubes. The selected cubes are highlighted on the display. The user can also synchronize the 2D and the 3D visualization zones.
  - The "Scale" tab ("S", Fig. 2): It provides the color scale (association between colors and protocols) used for the cones and the lines representing the packets.
- The "Messages" tab: Some status messages are printed under this tab. Headers of the displayed packets are also logged there so that the user can access detailed information if he wants to.
- The "Preferences" tab: The user can set some options and modify the behavior of the program. For instance, he can modify the color scale, set a filter to display only matching packets, adjust the length of time that packets are displayed on the visualization zones, ...
- The "Help" tab: To display some basic information about the prototype.

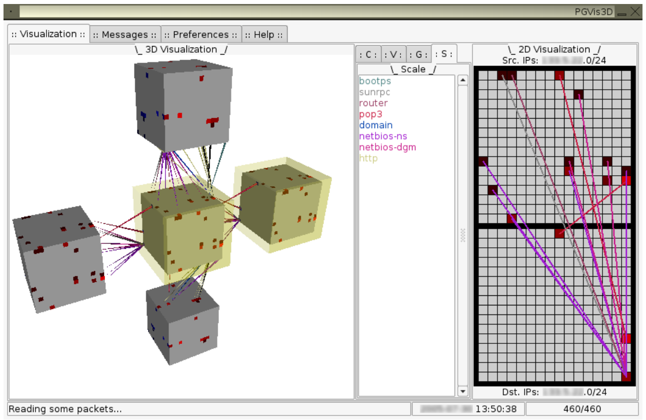
In addition to the controls provided on the GUI, the user can modify the viewpoint on the 3D visualization zone by zooming and rotating.

4.3 Use of the prototype

For the tests we chose to use layouts of five or seven cubes for the 3D visualization zone. However, it can be modified and adapted to the user's needs if necessary. In the initial state, the cubes on the left, middle and right of the screen all stand for the local network (a /24 network zone). The cubes on the top and bottom both stand for the global network (the /0 network zone). For the seven cubes layout, the additional cubes on the top-right and bottom-left both stand for a single host of the monitored network. We kept that configuration of the 3D visualization zone for Fig. 2, Fig. 3 and Fig. 4.

So the internal traffic of the local network is displayed between the left and middle cubes. It is also displayed between the middle and right cubes. The network traffic displayed between the bottom and middle cubes is the incoming traffic from the global network to the local network. The network traffic displayed between the middle and top cubes is the outgoing traffic from the local network to the global network. With the two additional cubes standing for the single host, the user can observe the traffic in both directions between this host and the local network, and between this host and the global network.

For Fig. 2, we used a small capture done on our local network from a connected host. The 2D visualization zone is set to display the internal traffic of the local network. The observed traffic is quite common, the local traffic is mainly constituted of broadcast activity. Regarding Fig. 3, we probed all the local network on the port 22 (SSH) from a local host. The portsweep is highly noticeable on the 3D visualization zone and the 2D visualization zone then enables the user to retrieve the exact source of that attack. For Fig. 4, we used the seven cubes layout. The traffic displayed contains a portscan of the host mapped on the two additional cubes. That portscan is also highly noticeable with cones drawn toward a lot of quadrilaterals of those two additional cubes. A remote host is trying to connect successively to several ports of the monitored host. On that figure, the transparency effect is activated and we can see the cones standing for the captured packets progressively vanishing on the 3D visualization zone.



Src. IPs: [redacted].0/24

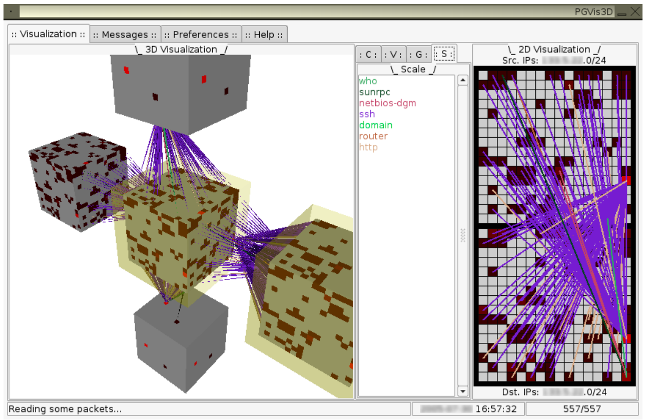
Dst. IPs: [redacted].0/24

Reading some packets...

[redacted] 13:50:38

460/460

Figure 2: Display of some usual network traffic on the prototype.

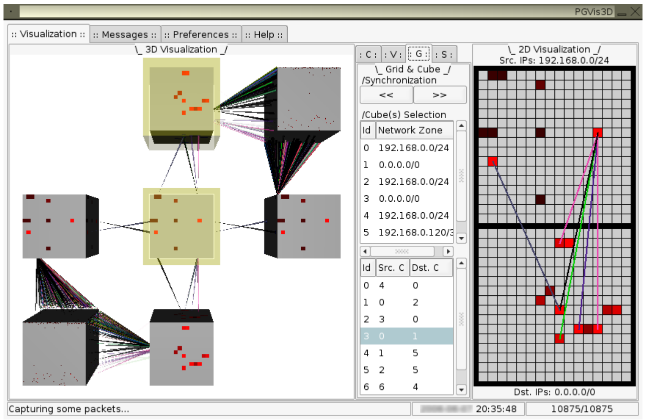


Src. IPs: [redacted].0/24

Dst. IPs: [redacted].0/24

Reading some packets... | [redacted] 16:57:32 | 557/557

Figure 3: Network scan from an internal host.



/Cube(s) Selection

Id	Network Zone
0	192.168.0.0/24
1	0.0.0.0/0
2	192.168.0.0/24
3	0.0.0.0/0
4	192.168.0.0/24
5	192.168.0.120/3

Id	Src. C	Dst. C
0	4	0
1	0	2
2	3	0
3	0	1
4	1	5
5	2	5
6	6	4

Src. IPs: 192.168.0.0/24

Dst. IPs: 0.0.0.0/0

Capturing some packets... | [redacted] 20:35:48 | 10875/10875

Figure 4: Portscan of a local host.

5. CONCLUSION

This paper introduces a visualization design combining both 2D and 3D representations of the network traffic. This design was built trying to solve some scalability and usability issues that we had with a previous design. A prototype was made based on that improved design in order to test it. We used this prototype not only to display several network traffic dumps but also to visualize network traffic in real time. We were able to detect several patterns corresponding to abnormal activity with the help of the prototype. Using this kind of visualization system really simplifies the detection of such patterns in the data compared to classical textual-based techniques. The proposed visualization design has proven to be more scalable through the 3D representation of the network traffic which can be adapted to the user's needs. Interactively combining both 2D and 3D representations lets the user finely control what he is visualizing. We believe that using such combinations of several linked representations of the network traffic can significantly improve the efficiency of the monitoring task and the overall understanding of the relations between the different hosts communicating. We also believe that this understanding is one of the keys to the detection of unusual behavior.

6. FUTURE WORK

The current prototype includes all the basic functionalities corresponding to the proposed visualization design. However, some further functionalities can be added to simplify its use. For instance, we plan to add a history of the network zones that were displayed on the 2D visualization zone to provide a quick access to them. We also plan to improve the management of the 3D visualization zone to enable the user to easily modify the disposition and the number of cubes in order to meet his needs (the current system being quite complex). We intend to conduct a user evaluation of the prototype once it is finalized. Another point we are interested in is the adaptation of our visualization design to the IPv6 address space as it is to replace the IPv4 system.

7. REFERENCES

[1] Etherape. `http://etherape.sourceforge.net`.

[2] Gtk+ library. `http://www.gtk.org`.

[3] Libpcap library. `http://www.tcpdump.org`.

[4] R. Ball, G. A. Fink, and C. North. Home-centric visualization of network traffic for security administration. In *VizSEC/DMSEC'04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 55–64, New York, NY, USA, 2004. ACM Press.

[5] A. Komlodi, P. Rheingans, U. Ayachit, J. R. Goodall, and A. Joshi. A User-centered Look at Glyph-based Security Visualization. In *VizSEC'05: Proceedings of the IEEE Workshops on Visualization for Computer Security*, pages 21–28, Washington, DC, USA, 2005. IEEE Computer Society.

[6] S. Lau. The Spinning Cube of Potential Doom. *Commun. ACM*, 47(6):25–26, 2004.

[7] E. Le Malécot, M. Kohara, Y. Hori, and K. Sakurai. Grid Based Network Address Space Browsing for Network Traffic Visualization. In *Proceedings of the 7th IEEE Information Assurance Workshop*, pages 261–267, Washington, DC, USA, 2006. IEEE Computer Society.

[8] J. McPherson, K.-L. Ma, P. Krystosk, T. Bartoletti, and M. Christensen. PortVis: a tool for port-based detection of security events. In *VizSEC/DMSEC'04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 73–81, New York, NY, USA, 2004. ACM Press.

[9] A. Oline and D. Reiners. Exploring Three-dimensional Visualization for Intrusion Detection. In *VizSEC'05: Proceedings of the IEEE Workshops on Visualization for Computer Security*, page 14, Washington, DC, USA, 2005. IEEE Computer Society.

[10] B. Shneiderman. The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations. In *VL*, pages 336–343, 1996.