Visualization for Cybersecurity

Kwan-Liu Ma
University of California, Davis

Networked computers have become an integral part of our everyday life, used for a variety of purposes at home, in the workplace, and at schools. They are so ubiquitous and easy to access that they are also vulnerable. Any computer exposed to the Internet is likely to be regularly scanned and attacked by both automated and manual means. Both organizations and individuals are making every effort to build and maintain trustworthy computing systems.

The main strategy is to closely monitor and inspect network activities by collecting and analyzing data about the network traffic and the trails of system usage. The analysis usually requires large amounts of finely detailed, high-dimensional data to enable analysts to uncover hidden threats and make calculated predictions in a timely fashion. The traditional, signature-based and statistical methods are limited in their capability to cope with the large, evolving data and the dynamic nature of the Internet.

Helping to solve cybersecurity problems

Visualization proves effective to aid in understanding large, high-dimensional data commonly found in many demanding applications such as large-scale scientific simulations and biomedicine. There is thus a growing interest in the development of visualization methods as alternative or complementary solutions to the pressing cybersecurity problems. The challenge is to develop new visual representations, layout methods, user interfaces, and interaction techniques that can effectively facilitate visual data mining, interrogation, and communication of the vast amounts of cybersecurity information.

Visual data analysis is inherently an iterative process, where each iteration provides more insight into the data being shown. A typical example of this process occurs with any type of overview + detail visualization. Patterns in the overview tend to direct what the user chooses to view in more detail, and the detailed view can provide insight on regions of the overview. This drill-down process, starting at a high semantic level and progressing to more detailed views, creates a feedback loop, which can lend itself well to visualizing the relationships between a large number of objects, such as port and network scans.[1,2] In most cases, different visual representations are needed for constructing these different views. In particular, each specific region of interest might be defined in a space of arbitrary dimensions. The challenge is thus to seek the best space and visual representation in that space for each type of analysis task. In addition, it is critically important to maintain an unbroken analysis context while drilling down into details. All these are topics of active research in information visualization.

The growing interest in developing visualization solutions for cybersecurity led to the convening of the first VizSEC Workshop, held in conjunction with the ACM Computer and Communication Security 2004 Conference. To foster greater exchange between the security and visualization communities, the second VizSEC Workshop was colocated with the IEEE Visualization 2005 Conference and the Symposium on Information Visualization. VizSEC 2005's technical program consists of eight long papers and eight short papers, attracting about 80 attendees.

In this issue

This special issue of *IEEE Computer Graphics and Applications* highlights the latest development and practice of visualization for cybersecurity. Among the five articles included, three are extended papers chosen from the VizSEC 2005 Workshop and two were selected from the special issue submissions.

The first article, "IDGraphs: Intrusion Detection and Analysis Using Stream Compositing" by Ren et al., presents a visualization system that couples data aggregation and interactive brushing for analyzing massive network traffic streams. The system attempts to reveal time-varying traffic patterns through stream compositing for the identification of correlated attacks.

The second article, "Hierarchical Visualization of Network Intrusion Detection Data" by Itoh et al., describes a hierarchical packing technique maximizing the density of the information in a visualization. Because the distribution of security incidents is visualized in the IP address space, the correlation between incidents and groups of computers can often be depicted.

The next article, "Visual Correlation of Network Alerts" by Foresti et al., discusses how to compare disparate events using interactive visualization based on a design unifying the presentations of different aspects of security information. The visual layout presented here effectively facilitates several different ways of interrogation.

 Published by the IEEE Computer Society

In "Countering Security Information Overload through Alert and Packet Visualization," Conti et al. present two complementary security-visualization systems designed according to a set of requirements obtained through surveying professional security operators. One system provides high-level overviews of intrusion detection alerts, while the other system gives detailed insights into packet-level network traffic.

The final article, "Focusing on Context in Network Traffic Analysis" by Goodall et al., shows how to seamlessly integrate contextual information into the temporal analysis of packet-level detailed events for reducing the cognitive burden on the analysts. Such focus plus context information presentation and exploration can only be realized using visualization.

These five articles only sample the abundant research efforts addressing the broader cybersecurity problems. However, I believe these articles show you the potential of visualization-based solutions and opportunities for further work. To learn about other advances, I encourage you to read the VizSEC 2004 and 2005 proceedings.[3,4]

I sincerely thank the authors who submitted their articles to VizSEC 2005 and this special issue. The high quality of the submissions made the selection process difficult. I am thus very grateful for the help I received from the 60 reviewers who gave careful and thorough evaluations of the articles. Thanks also to *IEEE CG&A* staff for their support and assistance to make possible this special issue. ■

References

1. C. Muelder, K.-L. Ma, and T. Bartoletti, "Interactive Visualization for Network and Port Scan Detection," *Proc. 8th Int'l Symp. Recent Advances in Intrusion Detection* (RAID), Springer Verlag, 2005, pp. 265-283.
2. C. Muelder, K.-L. Ma, and T. Bartoletti, "A Visualization Methodology for Characterization of Network Scans," *Proc. IEEE Workshop Visualization for Computer Security* (VizSEC), IEEE CS Press, 2005, pp. 29-38.
3. C. Brodley et al., eds., *Proc. ACM Workshop Visualization and Data Mining for Computer Security,* ACM Press, 2004.
4. K.-L. Ma, S. North, and B. Yurcik, eds., *Proc. IEEE Workshop Visualization for Computer Security*, IEEE CS Press, 2005.

Kwan-Liu Ma *is a professor of computer science at the University of California, Davis. His research interests span the fields of visualization, computer graphics, and high-performance computing, and he is presently leading research projects in both scientific visualization and information visualization. Ma has a PhD in computer science from the University of Utah. He received the 2000 Presidential Early Career Award for Scientists and Engineers for his work in large data visualization. He is a senior member of the IEEE and a member of the ACM. Contact him at ma@cs.ucdavis.edu or http://www.cs.ucdavis.edu/~ma.*