Demo: InViz – Instant Visualization of Security Attacks

Lucas Layman, Nico Zazworka
Fraunhofer Center for Experimental Software Engineering
College Park, MD, USA
{llayman,nzazworka]@fc-md.umd.edu

1. INTRODUCTION

InViz is a desktop tool for visualizing events from network applications, such as webserver application events or syslog events from network appliances such as routers or firewalls. InViz maps properties of events onto graphical objects that move across the screen in real-time as the events occur. For example, our Live Visualization maps types of requested files, the size of the HTTP response, and the HTTP response code to different shapes, magnitudes, and colors of the moving objects (see Figure 1 for an example of the interface). This visualization allows users to search for visual patterns in the flow of events in real time.

The Historical Visualization shows patterns of events over time sorted by event properties, such as the requesting IP. This sorting of events can reveal unique patterns of behavior from different IP addresses. InViz is controlled by the Timeline View and timeline controls, which function much like the standard controls on a DVD or DVR, allowing the user to control the display of the real-time information. The InViz cybersecurity visualizations combine concepts from glTail [1] and CodeVizard [2] to distill large amounts of information into a form more easily palatable to the user.

These visualizations leverage the human capacity for pattern recognition to identify anomalous events. By being able to process this information quickly, humans can also apply their contextual knowledge of the system to eliminate false positives, thus reducing the time to perform rapid/live forensics.

InViz is a functional prototype and has gone through a handful of internal releases, with a project release date of February 2013. A video demonstrating the capabilities of InViz may be found at: http://www.fc-md.umd.edu/inviz/.

2. DEMONSTRATION PLAN

We will briefly demonstrate the tool's capabilities on a real-life example take from Fraunhofer CESE's public-facing webserver. We will load the IIS 7.5 webserver application log file into InViz and demonstrate how InViz can quickly and easily identify abnormal patterns of behavior. We will highlight a naïve, script-based attack on our webserver that attempted to find a backdoor into an online email application. We will also show attempted accesses to administrative control panels for the phpMyAdmin application. We will also show some other potentially interesting patterns of behavior that are not, necessarily, attacks. We will, of course, limit what we show to the time allotted.

The goal of our demonstration is to focus on ease of use and understandability by security novices, rather than promulgate the tool as an attack detection or forensics silver bullet (which it is not).

Our takeaway is that we hope that InViz will be a useful tool for one or more of the following:

1) Narrowing the gap between attack notification and attack resolution by helping users understand log file data more quickly and accurately;
2) Lightweight analysis of webserver and router traffic by non-experts;
3) Training for security novices to identify attack patterns.

3. REFERENCES

[1] "glTail.rb – realtime logfile visualization", http://www.fudgie.org, 2007.

[2] N. Zazworka, C. Ackermann, "CodeVizard: a tool to aid the analysis of software evolution", 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM '10), Bolzano-Bozen, Italy, Sept. 16-17 2010

[3] U.S. Department of Homeland Security, "A Roadmap for Cybersecurity Research", http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf, 2009, pp. 90-98.

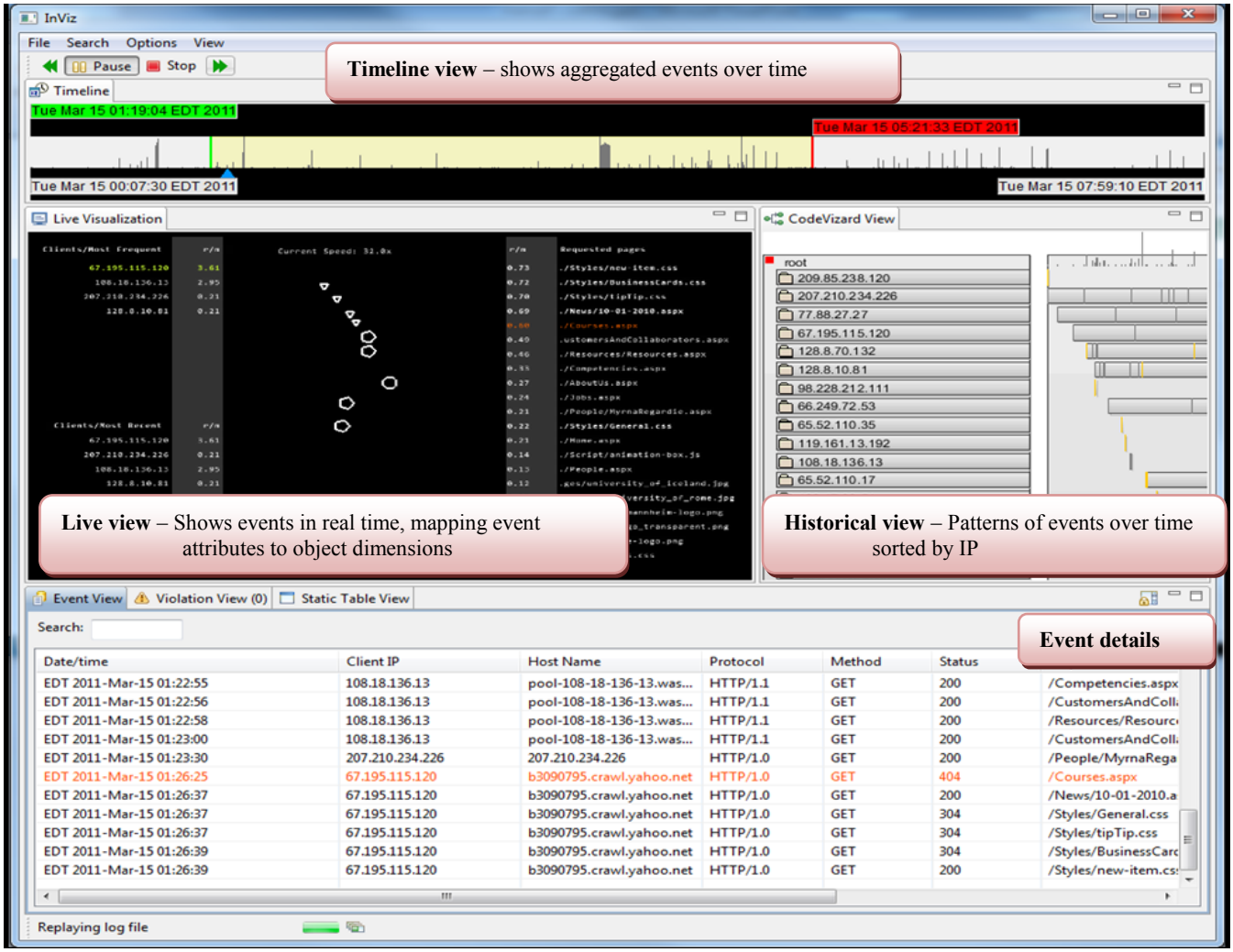

Figure 1. Screenshot of the InViz prototype processing IIS 7.5 webserver events