InViz: Instant Visualization of Security Attacks

Lucas Layman
Fraunhofer Center for Experimental Soft. Eng.
College Park, MD, USA
llayman@fc-md.umd.edu

Nico Zazworka
Fraunhofer Center for Experimental Soft. Eng.*
Frankfurt am Main, Germany
zazworka@gmail.com

ABSTRACT

The InViz tool is a functional prototype that provides graphical visualizations of log file events to support real-time attack investigation. Through visualization, both experts and novices in cybersecurity can analyze patterns of application behavior and investigate potential cybersecurity attacks. The goal of this research is to identify and evaluate the cybersecurity information to visualize that reduces the amount of time required to perform cyber forensics.

Categories and Subject Descriptors

K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*security*

General Terms

Security

Keywords

cybersecurity; visualization; log file; real-time analysis

1. CHALLENGES IN ATTACK MONITORING

Network cybersecurity attacks take on many forms, from network breaches to denial-of-service attacks to insider threats exfiltrating sensitive data. A 2010 study by Verizon and the U.S. Secret Service found that 98% of data theft took place on network servers, and that 86% of victims had evidence of the breach in their log files [**?**]. Despite the presence of such evidence, most victims did not find the evidence of a breach until it is too late (see Figure **??**).

The lag time between attack, detection and containment can be attributed to shortcomings in automated cyber defense systems and the challenges facing human users in investigating cyberattacks. The volume of network and log file information requires automated analysis solutions for detecting cybersecurity attacks. These automated systems are useful for processing large amounts of esoteric information, but, a human agent (e.g. an IT administrator) must often step in to verify or investigate an attack in detail, usually by examining log files. The tools to support log file investigation are often primitive, often no more sophisticated than a text editor or Microsoft Excel [**?**]. Much current cybersecurity research focuses on automated detection of anomalous events or defensive practices, often ignoring how to support the humans performing cyber forensics.

2. VISUALIZATION TO SUPPORT ATTACK MONITORING

The objective of this research is to identify, define, and evaluate graphical representations that are useful for investigating attacks in log files. Just as researchers investigate what information to show in an aircraft controller's display, fundamental research is needed to identify the ideal information display for a security expert (or novice) monitoring and investigating a potential security attack. Multi-dimensional information is required for a person (or automated agent) to verify an attack in real-time.

To illustrate our cybersecurity visualization concepts, Fraunhofer CESE has created an initial research prototype called InViz – Instant Visualization of cybersecurity attacks (Figure **??**, `http://www.fc-md.umd.edu/inviz`). These InViz cybersecurity visualizations combine concepts from glTail [**?**] and CodeVizard [**?**] to distill large amounts of information into a form more palatable to the user.

InViz transforms individual lines from a web server log file (easily adaptable to other formats) into objects that traverse the screen in real-time as the log file lines are written. The size, shape, and color of the animated objects correspond to attributes of the log entry: size is the number of bytes sent, shape is the type of file (e..g, media vs. HTML), and color reflects status code. Log event details are displayed in a table at the bottom. A timeline at the top shows the history of activity seen in the log file. InViz uses a DVD/DVR metaphor for playing the events in real-time: users can play, pause, stop, and fast forward. Users can also specify where in the timeline they would like to start and end. InViz resolves IPs to hostnames automatically, and allows users to specify strings that are highlighted (e.g., known attack strings, hex characters). Finally, a user can filter on, highlight, or ignore events from particular requesters. A demonstration video of InViz's capabilities can be seen at `http://www.fc-md.umd.edu`.

*Nico Zazworka is now with Elsevier Information Systems GmbH

HotSoS'14 April 08 - 09 2014, Raleigh, NC, USA
ACM 978-1-4503-2907-1/14/04
http://dx.doi.org/10.1145/2600176.2600191.

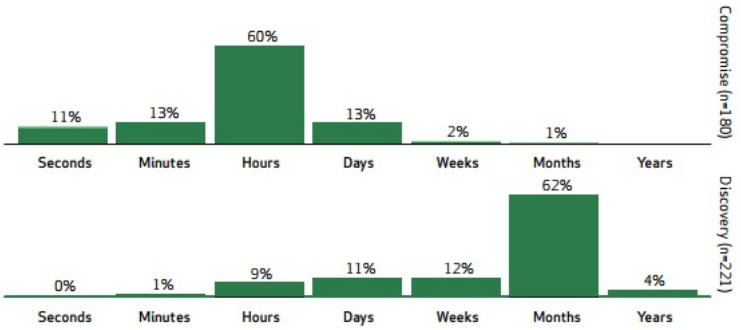

Figure 1: Typical times to detect and contain a security attack. [?]

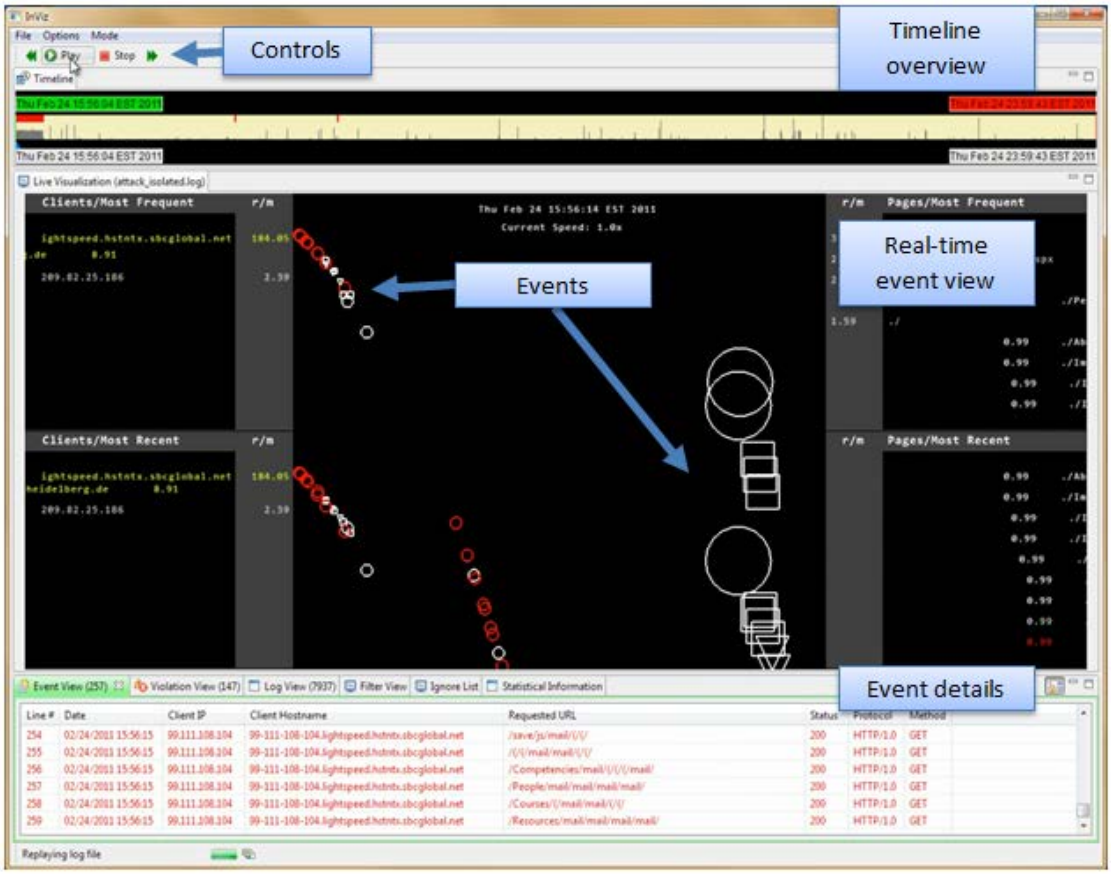

Figure 2: Inviz screenshot

3. ACKNOWLEDGMENTS

This research was sponsored by a Fraunhofer USA special funds grant. The authors would like to thank the following individuals who have contributed to the development of this tool: Manuel Schweizer, David Diffo, Jonathan Herdt, Linda Ramisch, Marcel Schwarzmann, and Marcel Sinn.

4. REFERENCES

[1] G. A. Fink, C. L. North, A. Endert, and S. Rose. Visualizing cyber security: Usable workspaces. In *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*, pages 45–56, 2009.

[2] E. Simonsen. glTail.rb - realtime logfile visualization. `http://www.fudgie.org`, 2007.

[3] Verizon. 2010 Data Breach Investigations Report. `http://goo.gl/28pPGM`, 2010.

[4] Verizon Risk Team. 2013 Data Breach Investigations Report. `http://www.verizonenterprise.com/DBIR/2013/`, 2013.

[5] N. Zazworka and C. Ackermann. CodeVizard. In *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement - ESEM '10*, page Article 63, Bolzano, Italy, Sept. 2010.