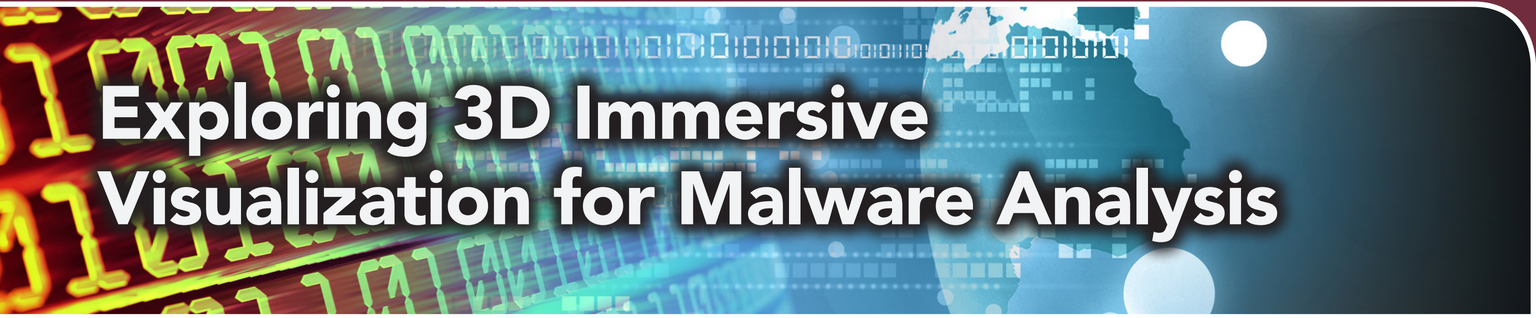
MISSISSIPPI STATE UNIVERSITY

HIGH PERFORMANCE DATA ANALYTICS

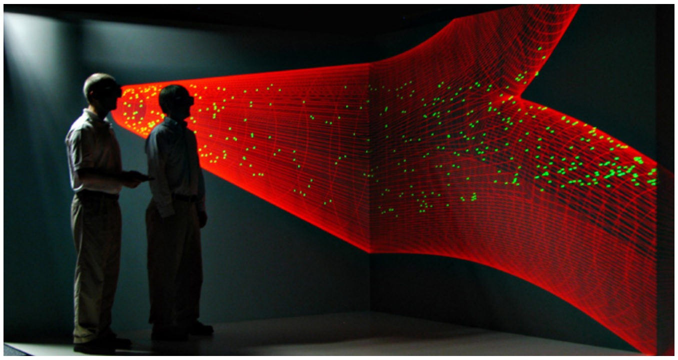


Exploring 3D Immersive Visualization for Malware Analysis

CHALLENGE

In our highly digitized world, protecting data stability and security is crucial. Protection entails understanding and preventing potential malware threats that could compromise sensitive and confidential information.

The productivity of malware analysts is limited by screen space and lack of visual support to help identify and track patterns. Viewing malware on a two-dimensional monitor is much like looking at the sky through a set of binoculars—one can only see a small section at any given moment. However, bigger displays and more pixels will not solve all issues. To understand and reverse-engineer malware, it is important to analyze the code in a context-rich environment including the code itself, the code block structure, memory accesses, cross references, and more. This project addresses current malware analysis issues by investigating different ways of integrating contextual information into a single three-dimensional (3D) display for improved malware analysis.



This 3D visualization system interacts with a disassembler/code analyzer that can be displayed in multiple virtual realitysystems like the CAVE environment.

> Developing 3D immersive and interactive visualization system for malware analysis

CURRENT PRACTICE

Analysts examine malware by converting binaries into human-readable assembly language and stepping through code using programs such as IDA Pro and Radare. While graphical interfaces do exist, limited screen space and visual tools place large cognitive demands on analysts. Current methods of analyzing and navigating disassembled code of complex cyber data can be overwhelming to an analyst who identify patterns, operations, and functions within the disassembled code while keeping track of patterns, operations, and functions that cannot be displayed simultaneously.

TECHNICAL APPROACH

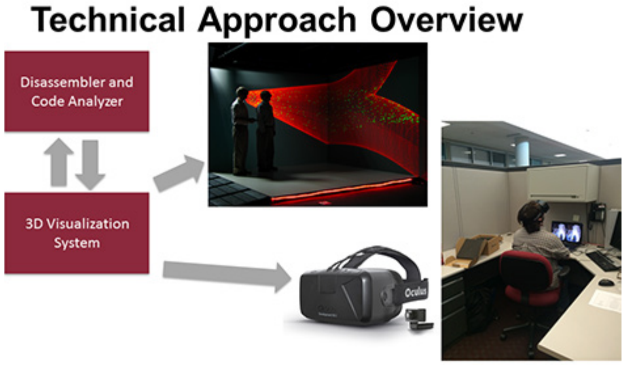
We leverage 3D immersive visualization to address challenges of analyzing and navigating disassembled code of complex cyber data. We hypothesize that utilizing 3D immersive displays will 1) diminish the screen real estate issue, 2) help users find information quickly and accurately within a context-rich environment, and 3) support analysts' efforts of grouping and classifying malware. Our approach focuses on six subtasks: data preparation, multi-level exploration, comparative visualization, interaction techniques, immersive visualization hardware, and evaluation.

Initial development and evaluation of the malware visual analysis system will occur in the Mississippi

State High Performance Computing Collaboratory Virtual Environment for Real-Time Exploration (VERTEX), because of its support for collaborative-viewing of immersive visualizations. The VERTEX is a cave automatic virtual environment-(CAVE)-like display that tracks user movement and is controlled by a handheld device. While the collaborative nature of the VERTEX makes it suitable as a development and training platform, cost and size make it less than ideal for wide-scale deployment to individual malware analysts. For deployment of the immersive static malware analysis system, we are exploring the Oculus Rift, an affordable wearable display. Both displays have a large field of view that supports the incorporation of more accessible data.

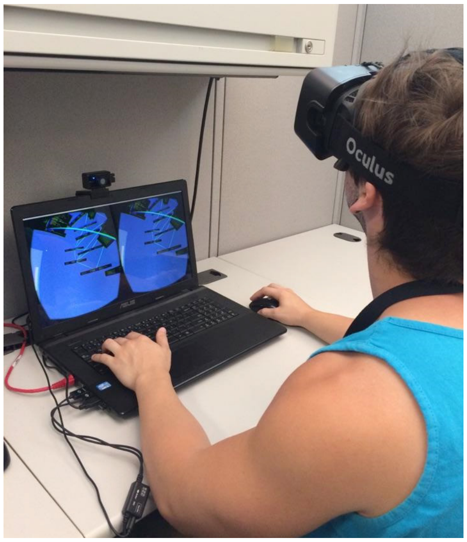
In a large-scale system with multiple data sources, developing techniques to interact with and navigate through the data is necessary. This effort will use tracking devices for the development of 3D gestures that can be used in concert with analog and digital controls to explore malware data in an immersive 3D environment.

To gauge the performance of the 3D visualization, evaluations will be conducted with expert users. We aim to answer three questions in these evaluations: 1) Does 3D immersive display improve the human understanding of the malware data? 2) Do interactions including the tracking and the 3D gestures facilitate understanding and collaboration? 3) How effectively can the users gain insight from their malware data with the 3D immersive display? Alternative malware analysis methods will be compared to our 3D immersive visualization system.


Technical Approach Overview

IMPACT

Our proposed systems will address issues surrounding visualizing the large amount of code per malware sample, and ultimately, visualizing the larger phylogeny of multiple samples. The development of this system complements the work already underway in the Cyber Phylogeny MSU/PNNL project led by Dr. Wesley McGrew, and will provide part of the interface that analysts will use to work hands-on with the Cyber Phylogeny results and data. Additionally, similar to our success developing practical tools and training in other domains, we anticipate the immersive 3D malware analysis system will serve as a platform for training new analysts.



Our system also can be used and displayed using the Oculus goggles on a Desktop platform.

Contacts

Jean Mohammadi-Aragh
Assistant Research Professor
662.325.2042
jean@dasi.msstate.edu

Derek Irby
Research Associate
662.325.8885
derek@gri.msstate.edu

Funding provided by a grant from Pacific Northwest National Laboratory.