CyberViz: A Tool for Trustworthiness Visualization of Projected Cyber Threats

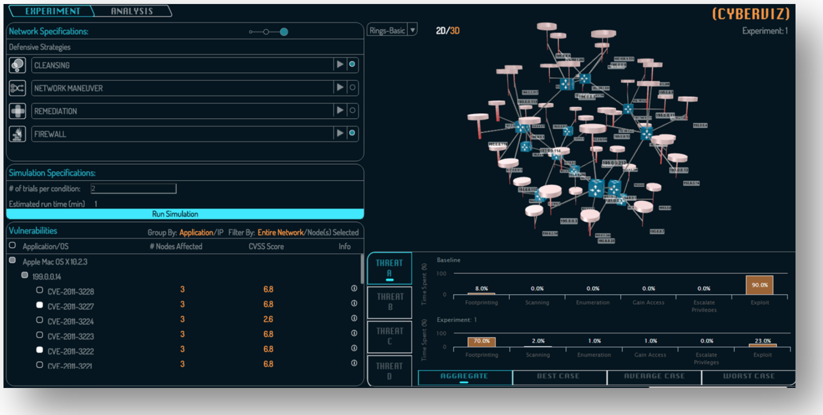
Ewart de Visser*[1], Alix Dorfman[1], Marvin Cohen[1], Niraj Srivastava[2], Christopher Eck[2], Suzanne Hassell[2]

Perceptronics Solutions, Inc.[1]
Raytheon, Space and Airborne Systems[2]

Today's cyber operator is faced with the daunting task of making sense of numerous data sources in a still poorly understood high-stress domain. Automated detection and decision support tools can help an operator, but such tools may suffer from imperfect recommendations and diagnostics. There is thus a need to develop visualizations and apply them to relevant data to understand and verify these automated recommendations. Trust cues are information data visualizations that can be used to make a judgment about the trustworthiness of data, a hypothesis or a recommendation by an automated agent. Trust cues can help improve attitudes of operators so that the *perceived* trustworthiness of a network or automated agent matches its actual trustworthiness, thus yielding *calibrated trust*. Our goal in this work was to develop such visualizations for relevant cyber data and automated recommendations for network defense.

We used a cyber simulation tool that generates data to portray vulnerability within a network and provides recommendations about the best way to defend against attackers. Three novel visualizations, the DICON, Vulnerability Rings and Flexible 3D Network Displays, were used to show the location, uncertainty, and scale of a simulated network attack into a coherent visualization tool named CyberViz (see Figure 1). The *Decision Information Icon* (DICON) is a dynamic display designed to provide an "at a glance" representation of uncertainty about a hypothesis. Vulnerability rings are designed to show the risk of attack and vulnerability to each node in a virtual network and correspond to six defined stages of a cyber-attack. 3D networks displays are used to flexibly swap multiple dimensions onto nodes and re-structure the network to highlight the most relevant information. Using these displays, we effectively visualized stages of an attack, variability associated across attacker profiles, and re-configured the structure of the network to highlight the most vulnerable nodes. A small investigation examining the utility of CyberViz found that cyber security professionals rated the tool as intuitive, easy to learn, and useful.

Tools such as CyberViz can save time for cyber analysts by simulating the effectiveness of a defensive intervention and iterating on a solution before deployment into the operational network. Cyber analysts can also use the tool to visualize large datasets and discover new relationships between relevant variables. The visualizations used here can further save time by highlighting the most significant threat to a system allowing operators to detect anomalous behavior or the most significant vulnerability to their systems. In summary, CyberViz can assist cyber operators in performing critical diagnostics so that they can engage in proactive defensive strategies to prevent attacks and increase network resiliency.



# of trials per condition: 2

Estimated run time (min) 1

Group By: Application/IP Filter By: Entire Network/Node(s) Selected

○ Application/OS	# Nodes Affected	CVSS Score	Info
Apple Mac OS X 10.2.3			
199.0.0.14			
○ CVE-2011-3228	3	6.8	ⓘ
● CVE-2011-3227	3	6.8	ⓘ
○ CVE-2011-3224	3	2.6	ⓘ
○ CVE-2011-3223	3	6.8	ⓘ
● CVE-2011-3222	3	6.8	ⓘ
○ CVE-2011-3221	3	6.8	ⓘ

Figure 1 CyberViz Application