B32 Using Visualization of Digital Forensic Datasets to Develop Fraud Detection Algorithms

Kara L. Nance, PhD, PO Box 81225, Fairbanks, AK 99708; Stephen McCombie, PhD, Macquarie Univ, Center for Policing, Intelligence and Counter-Terr, Macquarie, AUSTRALIA; and Ben Reardon, BS, Dataviz Australia, Macquarie, AUSTRALIA*

After attending the presentation, participants will have an understanding of abductive reasoning through visualization and an appreciation of the potential to leverage human visual processing with algorithmic development to detect and deter anomalous activities.

This presentation will impact the forensic science community by adding valuable tools and approaches to detecting anomalies in large data sets through visualization and the potential for using this information proactively to detect and prevent crime.

Mitigating card-present fraud through digital forensic analysis can be easy when the behaviors associated with the actions have been identified. The situation is much more challenging when one is not sure for what one is looking for. The human mind has a powerful ability to identify visual anomalies in large datasets. As part of a defense-in-depth strategy, this can contribute to the evolution and refinement of rule sets that facilitate the detection of the crime prior to the cash-out phase of the illegal operation. This presentation investigates the application of visualization, combined with human abductive reasoning, to the problem of identifying some behavioral characteristics of card-present fraud. It then demonstrates the behavioral characteristics in a digital forensics context, and demonstrates how this knowledge can be used to guide the evolution of analytical tools to help protect our digital assets.

The digital footprint left by individuals as they interact with technology throughout the day is astounding. As the use of Automated Teller Machine (ATM), credit, and debit cards becomes increasingly ubiquitous, the associated vulnerabilities make them more and more prevalent targets for cybercriminals. After a crime has been committed and identified, it may be possible to encode the observed information to develop an algorithmic approach to solving the problem. Since an algorithm is a step-by-step method to solve a problem or reach a goal state, clearly the process for solving the problem must be well understood. This works well when the problem is one that has been encountered, studied, and analyzed. What happens when new situations occur that are not expected? In this case, humans are able to reason abductively, and also excel at visual pattern recognition. This provides them with the ability to identify issues that are new.

Visualization is an excellent approach to facilitate these efforts as it allows the human analyst to see and evaluate datasets even when they do not know for what they are looking. Harnessing the power of visualization can provide a valuable tool in the arsenal to detect ATM usage anomalies including skimmed (counterfeited) card fraud. This presentation demonstrates how visualization techniques can be applied to couple the computational power of today's computers with the ability of the human mind to process images and reason through uncertainty. The example provided starts with abductive reasoning and is then analyzed and discussed reflexively. The intent is to demonstrate the value of visualization, in this case using parallel coordinates as a visualization tool, to identify anomalous patterns in data. The analysis of the findings can lead to the tuning of algorithmic tools to detect, and potentially prevent, future attacks using the same *modus operandi*.

This presentation will use a type of card-present fraud as an example to show how behaviors described can be detected through visualization of ATM datasets that are already being collected as part of standard operating procedure. Visualizing this data allows the human user to identify anomalies and use this information to contribute back to the design of effective algorithms to mitigate the threat. The objective of this form of data visualization is to identify and study criminal *modus operandi* in complex datasets and then use this information to design realistic automated rule sets for use in real time analytics tools. Incorporating visualizations into fraud control frameworks will help design new tools and mature existing tools and, thus, will be a positive step forward for practitioners in the cyber crime prevention field. While there is much work remaining in this problem domain, this presentation demonstrates how anomalies can be identified and then coupled with the behavioral characteristics in context. The resulting information can be used to guide the evolution of analytical tools to help protect our digital assets.

Visualization, Digital Forensics, Fraud

 ** Presenting Author*