Visualization of ATM Usage Patterns
To Detect Counterfeit Cards Usage

Ben Reardon
Dataviz Australia
ben.reardon@dataviz.com.au

Kara Nance
Computer Science
University of Alaska Fairbanks
klnance@alaska.edu

Stephen McCombie
Center for Policing, Intelligence and Counter-Terrorism. Macquarie University
stephen.mccombe@mq.edu.au

Abstract
People relish the flexibility of being able access their monetary assets when and where they need them. The abundance of cards able to withdraw funds from Automatic Teller Machines (ATMs) has not gone unnoticed by the cybercriminal element. Means for skimming and cloning cards exist and the market continues to grow. While the methods for obtaining access to another’s funds vary greatly, there are cases in which visualization of a class of card-present fraud can combine the visualization with the powerful abductive reasoning capabilities of the human mind to help identify the threat. 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 paper discusses card-present fraud and provides an example of how visualization techniques, coupled with human abductive reasoning, can be used to guide the evolution of analytical tools to help protect our digital assets.

1. Introduction

As the use of Automated Teller Machine (ATM), credit, and debit cards becomes increasingly ubiquitous, the associated vulnerabilities make them a more and more prevalent target 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 what they are looking for. Harnessing the power of visualization can provide a valuable tool in the arsenal to detect ATM usage anomalies including skimmed (counterfeited) card fraud. Further this detection can take place prior to the final “cashing out” portion of the crime chain, thereby providing valuable information to help protect consumers from unauthorized access to their digital assets. This paper 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 future attacks using the same Modus Operandi.

2. Background

ATM card skimming is a significant and growing problem for banks globally. The Australian Payment Clearing Association (APCA), reported in June 2010 that skimming fraud on Personal Identification Number (PIN)-only debit cards increased from around AUD$5m in 2008 to AUD$17.5m in 2009 [1]. Aite Group estimated counterfeit card fraud cost the United States US$1.349 Billion in 2008 [2]. The UK payments Association (ACMA) reported in 2010 that losses to counterfeit plastic cards in the United Kingdom between 1999 and 2009 were over UK£1.2 Billion [3]. However it is notable that there was a drop of some 52% in losses to counterfeit cards in 2009 over 2008 in the United Kingdom. This was mainly due to the introduction of chip and pin technology making the successful use of counterfeit cards far more challenging for cybercriminals.

Unfortunately countries such as Australia and New Zealand that do not use chip and pin in ATMs have seen the migration of that fraud to them as gangs now target
non-chip and pin countries for fraud. Also due to the nature of the global ATM system, cards protected by chip and pin in the United Kingdom can be counterfeited without the chip and used in non-chip and pin ATMs elsewhere. The global nature of the problem is demonstrated in Royal Bank of Scotland (RBS) Worldpay case in 2010 [4]. While not necessarily typical of the ATM frauds, with more extensive planning than is normally seen, it still demonstrates the global scope for losses in this area. Some US$10 Million was stolen through ATM fraud to counterfeit cards in just 12 hours from 2100 ATMs in 280 cities across US, Ukraine, Italy, Hong Kong, and a number of other countries. The architects were from Eastern Europe with a large number of accomplices in other countries. While the Estonian members of the conspiracy have been jailed, with one being extradited to the United States, two of the main Russian offenders, despite being arrested and prosecuted, only received suspended sentences and fines (albeit significant) [11]. Another of the architects, from Moldova, is still at large. Investigation and prosecution of offenders in these types of attacks given their International nature therefore is problematic and often provides little disincentive to other criminals from similar jurisdictions.

While it would seem a simple solution to migrate all cards and card readers to chip and pin, it is so expensive that there are no short term plans for such a global changeover. Even Australia, with its high security standards for banking, reportedly did not having a single chip and pin ATM in the entire country as of September 2010 [5]. This situation is despite pleas by senior law enforcement, including the head of the New South Wales Fraud Squad Superintendent Col Dyson at the Australian National Identity Crime Symposium in 2010, to make this changeover a priority [6]. While the total global losses are difficult to assess, it is clear that cybercrime involving cards is becoming increasingly profitable and thus, increasingly common. The adversary is no longer a single hacker targeting an individual’s account, but rather organized crime efforts to exploit large numbers of cards for profit.

Many of the approaches to solving these problems rely on the adaptation of solutions from other problem domains. Traditional approaches to this problem include statistical approaches, such as data mining, and may draw on the rich body of knowledge that is constantly evolving using artificial intelligence techniques. These methods generally rely on the computer processing the data, potentially with some expected outcome. Unfortunately, many of the approaches to addressing this issue involve reactive techniques utilizing data processing after the adversary has obtained the asset. This involves detecting a compromise after it has occurred and then beginning an investigation at that point. This approach, while valid and valuable, uses a crime-solving rather than crime-prevention approach. They also rely on computer systems, which while programmed by humans, do not take advantage of the ability of humans to process visual data.

3. Data Visualization

While it is widely recognized that data visualization is a valuable tool for processing large quantities of increasingly complex data and is an emerging, enabling field that feeds business intelligence, there are some challenges associated with the evolution of visualization. One of the limiting factors in the evolution of data visualization is the nature in which the advances generally take place. A researcher in a particular domain has data that can benefit from analysis of a visual interpretation of the data. The researcher generally deals with other researchers in the same field. The researcher may utilize an existing visualization technique used in his field or perhaps, if technically savvy, may develop a new visualization technique. This new technique is likely only to be viewed and shared within the same research domain.

Visualization is generally an “add-on” or “value-added” product within a domain. This evolution has happened due to the enabling factors that 1) researchers tend to visualize domain-specific data based on existing domain-specific data visualizations and 2) most researchers are not experts or developers of visualization tools. As a result, the valuable visualization techniques that could benefit many researchers may never make it outside of their very narrow disciplinary boundaries. This domain, specifically, has examined real world ATM use in a fraud context [7], an automated credit card fraud detection system based on neural network technology [8] and other models for visualization of card fraud data [9].

4. Card Fraud

Since the advent of credit and debit cards there have been criminal elements developing ways to defraud them. After the introduction of ATMs in the late 1970s, subsequent ATM fraud led to the integration of cameras into the ATMs, which were intended to identify the card user. Ironically at the time, these cameras also served to prevent customers lying about transactions they made rather than identifying criminals misusing their cards. Today however, these same cameras are an important tool to help identify skimming gangs, and are mentioned in the Future Consideration section of this paper.

There are two main types of card fraud, Card Not Present (CNP) and Card Present (CP) fraud. CNP transactions, which are relatively common on the Internet, is where the card details are supplied for a transaction, but the merchant or bank does not see the actual card itself during the transaction, hence the term card not present. Compromised cards are used to buy various goods and
services using telephone/mail order channels and more recently Internet channels. These losses are generally borne by the acquiring merchant and are therefore often seen as a business risk they accept. Currently banks operate various detection methods to identify CNP credit card fraud by profiling transaction and flagging for investigation those that fit a suspicious profile. Because of the nature of these transactions they can often be stopped before there is any loss, if proper rules are put in place that alert banks of such suspicious activity.

Card Present (CP) fraud on the other hand is where a stolen or counterfeit card is used. It is a particularly difficult problem where skimmed details are used on a counterfeit card in an ATM when the PIN has been compromised. Because of the real time nature of the cash transaction, it is difficult to do any meaningful profiling in time to prevent the actual loss from occurring. This research is intended to help with this particular weakness through visualization of these transactions to reveal the clear Modus Operandi of the skimming crime gangs.

5. Example CP Fraud

The primary focus of this research is centered on studying and hypothesizing criminal MOs and devising ways in which to use human visualization techniques to identify these activity patterns. This example demonstrates how the visualization of passive data can provide an inexpensive means to analyze past trends to predict future behavior and model rules to detect such fraud. The life cycle of an example card-present fraud is first presented to provide a context. This is followed by a discussion of the digital footprint that this type of crime leaves behind and examples of how data visualization can aid in the detection of triggers to stimulate action prior to the cashing-out step, thereby potentially preventing, rather than detecting the associated cybercrime.

5.1 Fraud Life Cycle

While the fraud life cycle can vary greatly depending on the techniques and objectives of the criminal, this example is presented as four discrete phases: the counterfeiting phase, the distribution phase, the reconnaissance phase, and the cashing-out phase. The overall objective of this research is to provide a means to detect potential misuse prior to the cashing-out phase.

The counterfeiting phase is the phase in which the information associated with the card in obtained presumably for nefarious purposes. In the case of cards with magnetic stripes, devices called “skimmers” are used to covertly copy the information held on the magnetic stripe. Hidden pinhole cameras are used in conjunction with skimmers, to capture the Personal Identification Number (PIN) of card owner. These devices can be deployed in a vast array of configurations, and can be extremely well disguised within fake shrouds that appear legitimate, such that a skimmer may go unnoticed even to the most astute card user. The devices may be installed on ATMs themselves, on Point Of Sale (POS) terminals, train ticket vending machines, and even on ATM foyer enclosures where customers must swipe a card to enter a semi-secure ATM queuing foyers. The technology can also include “Bluetooth” functionality that allows the transmission of the PIN numbers and magnetic strip data to remote sensors wirelessly, which further decreases the potential for detection. The underground market has developed environments where these devices are bought and sold at low cost as commodity items, making the devices accessible even to low level criminal groups.

With the information from the card now in hand, a working replica (clone) of the card can be made which can be used at an ATM machine to withdraw cash from the victim’s account. The cards can also be used for CNP fraud, however the cash option is often attractive and this makes counterfeit cards a popular commodity on the underground market.

The distribution phase is the stage in the fraud cycle where the cloned cards are distributed. Once these cards are counterfeited, the data may be bought and sold in underground forums to other crime groups who carry out subsequent steps of the crime chain. The underground economy supports groups to become specialized in any and all of these links in the overall crime chain. This model allows for crime groups to select activities based on a risk and reward that suits their skill level, risk appetite, and access to resources. The business model is not dissimilar to that of an organized crime environment such as in drug trading networks e.g., Drug Grower → King Pin → Global distributor → Mule network → Local distributor → Street seller → End user.

The purpose of the reconnaissance phase is to answer two primary questions for each cloned card 1) Is the card valid? and 2) How much cash is available? The answers to both of these questions can be accomplished, generally without attracting attention, from a low-volume ATM or an ATM in a quiet area. The collection of cloned cards is inserted (one-by-one) into an ATM along with the associated PIN. The associated request is for “Account Balance” and the resulting value is then recorded either by note, or writing the amount in ink onto the card itself. After this information has been collected for each card, the reconnaissance phase is complete and the cards are generally split up for the cashing out phase. This “batch processing” approach to reconnaissance, without associated withdrawals, minimizes the risk to the criminal, as mere possession of the cards is in many jurisdictions a lesser crime to possession and subsequent theft of account monies.

At this point, there is still no indication that there is anything amiss with the cards. Balances for a range of
cards from a range of banks have been checked. As we will see later, this point is the first and only real point where there remains hope of detecting counterfeit cards prior to the money being withdrawn.

The *cashing out phase* is similar to the reconnaissance phase, conducted potentially at late hours, and at quieter ATMs where there may be very few observers, if any at all. It is important to note that from the criminal perspective, this entire process is bank-brand agnostic. It does not matter to the criminal which bank owns the card or which bank owns the ATM used to cash out. The primary consideration for the criminal is selecting an isolated and recently stocked ATM, and presumably the lack of a surveillance camera is also of benefit.

Some important characteristics of the activity at this point include the following:

- The number (volume) of cards used at that ATM will be larger than usual.
- The amount withdrawn will be either the minimum of 1) the maximum allowable daily limit set per card (e.g., $300) or 2) An amount close to the amount left on card, thus emptying the account of funds.
- The first choice for "note stock" used to tender the withdrawal amount will likely be the larger stock amount, until of course this stock is depleted (e.g., in Australia, stock notes are $20 and $50. In the U.S. it varies with location, but is generally $20.). Thus the $50 notes in Australia will run out at a much faster rate than normally would be the case.
- The transactions will be made in rapid succession, with minimal waiting time in between.
- There will be no non-withdrawal transactions during this session.
- After a flurry of transactions, the ATM activity will drop off dramatically returning to normal activity levels (may be zero).
- The same person will make all of these transactions on multiple cards. This is the case during both reconnaissance and the cashing out phase, and at first it seems like an obvious statement. However the significance of the benefits of detecting this with some form of "camera image hashing" is highlighted in the Future Considerations section of this paper.
- In the case of timed attacks, there may be this same activity across many ATMs potentially in different countries.

The cashing activity is distributed and executed quickly and likely in parallel at a many ATMs. This distributes the cashing activity and lessens the potential for detection by shortening the length of the cashing operation. This method does present a promising window of opportunity to identify the nefarious activity by detecting the unusual behavior. This behavior will be anomalous in both the card activity location (e.g., likely to be at an ATM far away from owners general sphere of usage) and for the ATM itself as far as volume levels and types of transactions.

The previous description of the fraud life cycle is the hypothesis put forward on which to test visualization techniques. There will likely be many other criminal Modus Operandi that will be evident upon further mapping of visual representations on ATM log data.

### 5.2 Digital Footprint

While the fraud life cycle present in the previous section is relatively easy to understand at a human level, it may not be quite so easy to develop computer systems to study and validate the criminal Modus Operandi. The strength of data visualization here is in the provision of human readable business intelligence tools that represent the digital footprint of ATMs usage patterns. ATMs log an extensive amount of data, which form the basis of this footprint. ATM network owners collect these logs for many reasons, including the following use cases:

- To support law enforcement.
- To support fraud investigations.
- To monitor own customer activity levels.
- To monitor foreign customer activity levels.
- To benefit own customers (e.g., support the placement of ATM's minimize costs).
- To maximize profit (e.g., increase usage by foreign customers).
- To monitor and alarm of ATM tampering (e.g., gas attacks, ram raids).
- To monitor malfunctioning ATMs.
- To monitor stock note levels, and automate the replenishment of same (e.g., company gets called to restock the ATM).
- To support charge back and network usage costs being apportioned back to the card issuer.
- To comply with regulatory requirements.

This valuable data, which is already being collected, can be used to detect the anomalies before the cash-out phase, thereby mitigating the threat.

### 5.3 Data Visualization

While the techniques and methods for visualization are varied, the attributes of this dataset can be easily demonstrated through the use of parallel axes per ATM,
and then extending this technique to the entire ATM fleet to create a heatmap style plot where the human eye is intuitively drawn to areas where the counterfeit Modus Operandi associated with anonymous ATM activity is exhibited. Parallel axes have been shown to be a valuable visualization tool to organize and digest a large number of multivariate events and, coupled with human visual analysis, have demonstrated a valuable method for abductive reasoning. [12, 13]

Due to non-disclosure arrangements, the data used for the visualizations in this paper is not associated with any particular ATM or bank, but rather has been constructed to illustrate typical common patterns of ATM usage and skimming activity.

Figure 1 demonstrates an example of a time-based visualization of an individual ATM, and includes both normal and anomalous behavior patterns. The axis on the left represents Balance Checks over time and the axis on the right represents Withdrawals over the same time scale. The edges (lines) connect transactions that use the same card. The unlabelled green edges at the top and bottom of the images are indicative of normal behavior. The red edges with the label "reconnaissance phase" in the center of the image indicate activities consistent with the Modus Operandi of both the reconnaissance and cash out phases as described in section 5.1. The activities on the left axis are consistent with the reconnaissance phase and the activities on the right axis are consistent with the cashing out phase. In this figure, both activities are shown as occurring on the same machine to demonstrate the dependency between the reconnaissance phase and the cash-out phase more clearly. The figure also demonstrates that we do not need to know any of the actual account holder details in order to identify the anomalous behavior.

Figure 2 extends the example to include a number of distributed ATMs. In some cases, we have retained the representation of reconnaissance and cashing-out occurring on the same machine to demonstrate the timeline and to reinforce the concept that, if the reconnaissance phase is detected, the cashing out phase can potentially be prevented. It is also important to note how the human brain can easily identify anomalies in this dataset, and how complicated it would have been to write the rule set to detect this anomaly without the associated visualization as a discovery tool. Algorithmic approaches...
are effective when the solution to a problem is well understood. Abductive reasoning approaches can aid in this initial understanding, which can help lead to stronger algorithmic solutions. When the datasets in this case are represented visually using a parallel axis approach, the mass of data facilitates identification of the following cases, which stand out to the human eye.

**Case 1:** In the reconnaissance phase of the fraud cycle, over 50 unique cards are used sequentially to obtain bank balances. These cards are not subsequently withdrawn from (in this dataset, at least). The cards may have been kept for later use, potentially when the accounts have more funds resulting from welfare payments or salary deposits.

**Case 2:** Over 50 cards are balance checked sequentially at one ATM, and these same cards are then used to withdraw funds at another ATM. The transaction amount started at the daily limit, and continued in the order of the card values. For example, the first three cards used originally had account balances over $1000, so the maximum daily amount was stolen:

- $1,000 withdrawn (maximum daily amount)
- $1,000 withdrawn (maximum daily amount)
- $1,000 withdrawn (maximum daily amount)
- $960 withdrawn (account now empty)
- $760 withdrawn (account now empty)
- $650 withdrawn (account now empty)
- ...
- $120 withdrawn (account now empty)
- $40 withdrawn (account now empty)

The order in which the cards are used indicates that the cards have been ordered from highest value to lowest. It is to the criminals’ advantage to withdraw the maximum amounts first, so if they are interrupted and need to make away quickly - they have maximized their takings.

![Figure 2 - ATM fleet activity](image-url)
Case 3: Similar to Case 2, except that the same ATM is used for balance checks and withdrawals. Note that the attack occurred close to midnight, so that potentially those higher value cards where the daily maximum was withdrawn could be attacked again just after midnight when the daily limit is reset.

Case 4: All cards are balance checked at one ATM, and cashed out at several ATMs in an organized and coordinated attack. The cashing phase may also be planned so as to maximize the cash note stock within the ATM by conducting the cashing out operation soon after the ATMs are replenished. Once again, the attack happened close to midnight to take advantage of doubling the takings for those cards where the maximum daily limit has been reached. It is easy to see how large volumes of cash are stolen in this way. A clear example mentioned earlier, is the RBS Worldpay case [4], which involved a heist of around US$10 Million, where 2100 ATM’s were used across 280 cities over a 12 hour period.

If we study the visualization model itself, there are very few key data pieces required to develop a reasonably meaningful model to start the journey. We need to know the time intervals that are represented on each axis. We need to know what type of transaction occurred, and from which unique cards these occur. We don’t really know the locations of the ATMs, but this is a valuable tool, and would increase the value significantly if the model including a geographic metric mapping aspect.

Visualization toolsets based on relevant and accurate data clearly augment and/or enable the creation and tuning of complicated rule sets to detect this anomalous behavior through log activity. When elements of a new, unseen problem are seen visually, humans are often able to discover correlations that may otherwise go unnoticed. This is because the human mind instinctively views the world in terms of patterns, which it recognizes based on memories of past experiences [10]. Based on this ability, we can use abductive reasoning to visually associate meaning with data. Using this powerful human technology, we can quickly determine accurate criteria for building an automated rule set that is consistent with these anomalies. Thus the human analysis of visualization can be part of an effective defense-in-depth strategy as a feedback mechanism to develop and refine rule sets in real time analytical tools.

5.4 Summary

The anomalous trends in figure 2 are even identifiable by a layperson, and certainly without even knowing what the data represents. This demonstrates an opportunity to apply abductive reasoning. Rather than understanding the data and looking for trends using a predictive model, the application of visualization demonstrated in this paper allows easy identification of candidate components of the data for further analysis. Thus, an anomaly is identified and then the cause is inferred, rather than looking for a cause and then determining the predicted result.

The previous section demonstrates how the type of card-present fraud 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.

6. Future Considerations

There is much more work to be done in this area. As new techniques for mitigating threats are developed, the Modus Operandi of the criminal elements adjust and become more sophisticated, so to continue to benefit from the high levels of profitability associated with cybercrime. Future research, development, and testing areas of focus include:

- Real-world applications of the visualization and defense evolutionary process for card-present fraud.
- Testing of theories by playback of ATM logs where skimming activity was identified.
- Develop ATM log visualization techniques to identify other Modus Operandi through abductive reasoning.
- Investigations into how the notion of anomaly detection visualization can be extended to the Card-Not-Present (CNP) form of card fraud.
- The application of anomaly visualization to detect Common Points of Compromise (CPP) where cards are initially compromised for the purpose of CNP fraud, or cloning and cashing out.
- Development of visualization techniques that take in data from global aggregate service provider’s ATM and POS device networks. This will deeply enrich and broaden the intelligence.
database beyond that available from a single bank’s ATM systems.

- Development of configurable risk-based alarm mechanisms, and extension of this approach to placing an auto-hold on cards suspected to be counterfeit, not dissimilar to those systems that are already used within the Credit Card CNP fraud space.
- Development of real time, dashboard style displays that can be used as functional decision support tools within Security Operations Centers.
- Development of the technology in the ATM camera whereby a non-identifiable hash or fingerprint of the person standing at the ATM would be produced. This technology would not identify a “person” so much as the overall sequencing of pixels representing the object (not the person, per se) that is directly in front of the ATM. This could distinguish repeat actions by a single individual from actions performed by a range of individuals, which would be additional supplementary information for detecting card fraud.

7. Acknowledgements

The authors wish to acknowledge the Honeyynet Project (http://www.honeynet.org), a leading international security research organization dedicated to investigating the latest online attack methods and developing open source security tools to improve Internet security.

8. References

http://www.ukpayments.org.uk/files/fraud_the_facts_201.pdf


Available from:


