Fear the Reaper: Characterization and Fast Detection of Card Skimmers

Nolen Scaife
University of Florida
scaife@ufl.edu

Christian Peeters
University of Florida
cpeeters@ufl.edu

Patrick Traynor
University of Florida
traynor@cise.ufl.edu

Abstract

Payment card fraud results in billions of dollars in losses annually. Adversaries increasingly acquire card data using skimmers, which are attached to legitimate payment devices including point of sale terminals, gas pumps, and ATMs. Detecting such devices can be difficult, and while many experts offer advice in doing so, there exists no large-scale characterization of skimmer technology to support such defenses. In this paper, we perform the first such study based on skimmers recovered by the NYPD's Financial Crimes Task Force over a 16 month period. After systematizing these devices, we develop the Skim Reaper, a detector which takes advantage of the physical properties and constraints necessary for many skimmers to steal card data. Our analysis shows the Skim Reaper effectively detects 100% of devices supplied by the NYPD. In so doing, we provide the first robust and portable mechanism for detecting card skimmers.

1 Introduction

Credit and debit cards dominate the payment landscape. Such cards have fundamentally transformed consumer behavior, from reducing the dangers of needing to carry large sums of cash to eliminating interaction between customers and employees at gas stations. Consumers now prefer to use such payment cards in the retail setting by a margin of more than three-to-one [52].

Almost as well-known as the cards themselves is the ease with which fraud can be committed against them. Attackers often acquire card data using skimmers – devices attached to legitimate payment terminals that are designed to illicitly capture account information. Once installed, skimmers are nearly invisible to the untrained eye and allow attackers to sell stolen data or create counterfeit cards. Such fraud is projected to reach over $30 billion by 2020 [5]. Moreover, even with the increased rollout of EMV-enabled cards, such fraud continues to grow, with ATM fraud increasing nearly 40% in 2017 [28]. Without reliable methods for rapidly identifying the presence of skimming devices, the frequency of such fraud is likely to continue growing.

In this paper, we design and deploy a device for detecting skimmers. We start by conducting the largest ever academic analysis of such devices. We then use the results of this analysis to develop the *Skim Reaper*, a portable, payment card-shaped device that relies on the intrinsic properties of magnetic stripe reading to detect the presence of additional read heads in a payment terminal. The Skim Reaper is inserted into the card slot and counts the number of read heads present in the slot; those payment terminals with more than one are identified as having a skimmer.

We address these problems through the following contributions:

- **Characterize and Taxonomize Recovered Skimmers:** We partnered with the New York Police Department's (NYPD) Financial Crimes Task Force and systematized the unique skimmers they identified across nearly 16 months. To the best of our knowledge, our taxonomy is the first large-scale academic examination of real skimmers. We then use this analysis to show that common advice to consumers to detect skimmers is *not* effective against modern skimming attacks.
- **Develop Portable Detection Tool:** We develop and present the Skim Reaper, a card-shaped device for detecting multiple read heads in a card slot. We explain the physics of reading magnetic stripe cards, then show how these can be used to both effectively detect read heads and prevent adversarial countermeasures.
- **Validate Tool Using Real Skimmers:** We first confirm the effectiveness of our system on a custom,

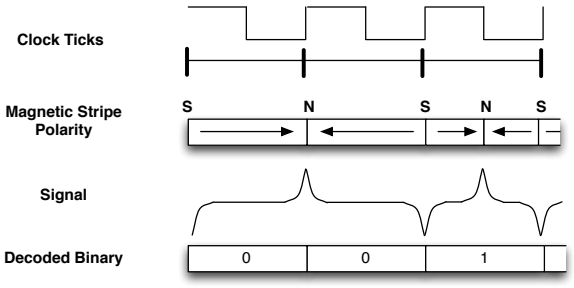


Figure 1: F2F Encoding: A polarity transition per clock cycle encodes a `0`, whereas two encode a `1`.

conspicuous 3D-printed skimmer. We then use 10 real-world skimmers to show that our system is robust against a wide variety of skimmer form factors.

The security of payment systems in general, and ATMs in specific, has long been studied in Computer Security [11]. Many members of the public even argued that such devices were already secure enough to use for national elections (although significant research in that space disagreed with such an assertion [32, 47, 45]). Unfortunately, these systems remain significantly vulnerable and require continued attention.

The remainder of the paper is organized as follows: Section 2 offers a primer on payment card readers and fraud against those devices; Section 3 analyzes and categorizes the skimming devices found by the NYPD's Financial Crimes Task Force in 2017; Section 4 details the design of the "Skim Reaper" detector; Section 5 provides experimental results against real recovered skimming devices; Section 6 discusses countermeasures and other insights; Section 7 examines related research; and Section 8 gives our concluding remarks.

2 Fundamentals of Card Reading & Fraud

2.1 Magnetic Stripe Encoding

Magnetic stripes store small amounts of data using frequency/double frequency (F2F) encoding. F2F stores both the clock and the data, allowing a reader to quickly synchronize and read the data when the card moves at an inconsistent speed (such as when being swiped). Figure 1 shows how decoding is performed: when the magnetic polarity change occurs within a clock cycle, the bit is a `1`. Otherwise, it is a `0`. Finally, the bitstream is decoded into plaintext characters containing the card data (e.g., name, account number, and expiration date). Data is stored on up to three adjacent tracks on a single stripe [29, 30], each having its own standard for character encoding and density.

2.2 Fraud

Magnetic stripe cards offer no inherent protection from duplication. All data contained on a card's tracks are written as plaintext, and an adversary with access to the magnetic stripe (e.g., with a skimmer) can create a legitimate card. These cloned cards, while magnetically distinguishable from the originals [4, 48], contain the same data as the originals.

To prevent the use of counterfeit cards, banks and payment networks added Card Verification Values (CVVs). CVV1 codes are part of the data on the magnetic stripe. This code prevents the card from being cloned with only knowledge of data printed on the physical card (e.g., the account number). However, if the adversary has access to read the card's magnetic stripe, the CVV1 code is easily cloned along with the rest of the stripe data. CVV2 codes are printed on the physical card and are often requested when making phone or online purchases (known as "card not present transactions"). This code is intended to prove possession of the original card. Adversaries can either acquire this code by recording PIN entry with a camera[1], through sites that sell card data with codes, and with compromised web browsers [35].

Once the adversary has obtained data and created a counterfeit card, the cards are "cashed out." When cashing out, counterfeit cards are used to either purchase goods (to be resold later) or to retrieve cash from an ATM. Once purchases for a given card are declined, the cards are discarded.

In the remainder of this paper, we focus on the problem of detecting acquisition of payment card data. Without this data, adversaries will be unable to perform card fraud.

2.3 Common Advice

Card skimming is a well-known crime, and advice aimed at protecting consumers is widespread. The most common suggestions are:

1. Look for signs of a skimmer.
2. Pull on the card reader.
3. Use a smartphone app to scan for skimmers with Bluetooth radios.
4. Use an EMV (Chip) card.
5. Use cash.

While seemingly helpful on their surface, many of these tips offer little in terms of specific steps. Beyond common sense, Tips 1 and 2 suggest that users know how payment devices should look and feel.

[1] Some credit and debit cards have the CVV2 printed on the face of the card and (for cards with the code on the back) some card acceptors allow the card to be inserted face down, allowing a camera with a view of the card to capture the code.

Location / Type	ATM	Gas Pump	POS Terminal	Total
Bank				**12**
Deep Insert	10			
Shimmer	2			
Gas Station				**6**
Internal		5		
Overlay	1			
Hotel				**3**
Overlay	2			
Wiretap			1	
Restaurant				**5**
Overlay	5			
Retail				**9**
Deep Insert	1			
Overlay	5		3	
Total	26	5	4	**35**

Table 1: The breakdown of skimmer BOLOs by the NYPD Financial Crimes Task force between 2016-Jul-14 and 2017-Nov-11. ATMs were the most widely attacked device using both deep-insert and overlay skimmers.

Tip 3 proposes the use of a smartphone-based app for detecting Bluetooth radios. Of all of the above tips, this is the most easily testable, and the strength of this tip can be evaluated based on an analysis of the relative use of Bluetooth radios by skimming devices.

Tip 4 suggests that users have the option to use a chip-enabled card; however, EMV deployment is far from universal. For instance, less than 7% of ATMs in New York City accept EMV [44], and ATMs in Europe with EMV enabled continue to see an increase in skimmers [34]. This is because EMV-enabled cards have a magnetic stripe as a backup, which attackers can still use to clone card data.

Finally, Tip 5 requires that users essentially abandon payment cards or fundamentally change their behaviors (e.g., instead of paying at the pump, go inside the gas station, wait in line and pay with cash). Security solutions requiring significant behavioral changes are unlikely to be successful.

We will use our observations in the next section to further evaluate Tips 1, 2, and 3.

3 Characterizing Real-World Skimmers

As we discussed, common advice for reducing the risk of being a victim of skimming is pervasive. These arguments are based on the detectability of single skimmer models and not on a complete understanding of skimming attacks. To the best of our knowledge, there has been no systematization of real-world skimmers, leading to a gap in our understanding of these devices and how they continue to be successful despite this advice.

To gain a better understanding of the skimmers found in practice, we partnered with the NYPD Financial Crimes Task Force and obtained their skimmer BOLOs[2] for the time ranging from 2016-Jul-14 to 2017-Nov-11. The 35 memos we obtained provide the location, type, and data retrieval method for *unique* skimmers discovered during this time. Table 1 shows the breakdown of each of the recovered skimmers. Multiple devices of the same campaign do not result in an additional BOLO. As a result, they provide clear insight into the variety of skimming technology confiscated by police in the New York City market. We explore these reports and perform the first large-scale characterization and breakdown of skimmers.

3.1 Taxonomy

In the skimmers discovered by the NYPD, we found five distinct installation points for skimmers in two categories: those that require only *external access* to the target device and those that require *internal access*. For external access, the skimmer can be installed without opening the payment device[3]; for internal access, the payment device must be opened (e.g., via key or drilling a hole). We further divide these into skimmer *types*, which for external-access skimmers consist of: those that fit on the magnetic stripe slot (overlays), those that fit in the magnetic stripe slot (deep-inserts), those that fit in the EMV slot (shimmers), and those that fit on the physical communication line (wiretaps). Figure 2 provides a diagram of an ATM with the placement of each type of skimmer.

3.1.1 External-Access Skimmers

Skimmers requiring no access to the internals of the target machine were the most common type of device recovered. These are the lowest-risk devices to deploy since they can be installed in seconds [54] and are difficult to identify without expertise.

Overlays were the most prevalent device discovered in our data set, comprising nearly half (46%) of the skimmers. These devices are placed on top of the card slot using a form factor custom-designed to match the target machine. The rear side of the overlay contains a magnetic read head, decoding and storage equipment, and a battery. Since the overlay sits atop the card acceptor, only millimeters exist between the new façade and

[2] "Be on the lookout:" These memos are sent out to inform other officers to watch for similar attacks.

[3] For simplicity, we refer to any device which accepts a consumer payment card (e.g., an ATM, POS terminal, or gas pump) as a *payment device* unless discussing a specific type of device.

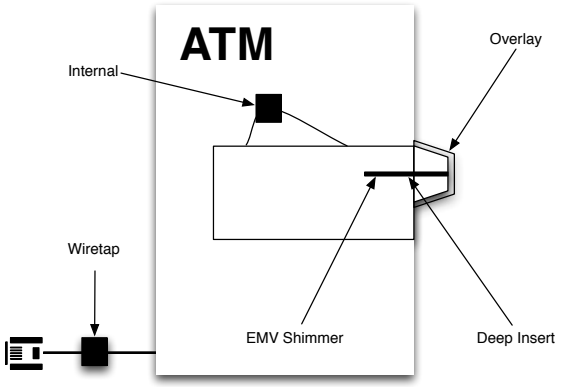


Figure 2: A cross-section of an ATM with skimmers having internal access (Internal) and external access (Overlay, Deep-Insert, EMV Shimmer, and Wiretap).

the original, so the adversary has little room to add additional features or battery capacity. Figure 3 shows a typical overlay skimmer. While common advice is to tug on these devices, our contacts inform us that the tape to hold it on is often strong enough to resist pulling the device straight off without a prying tool (such as a knife). This prevents the skimmer from falling off or being easily removed; these skimmers often cost hundreds or thousands of dollars each, so the adversary is motivated to keep the devices. Although Tip 2 may result in some success in detecting skimmers, this remains unreliable, invalidating Tip 2.

When the victim's card is inserted, an independent read of the card is performed, decoded, and stored. While we initially expected these devices to have wireless data retrieval capabilities, only 2 of the 16 devices had this capability. Our partners informed us that because these are battery powered and have limited space, the devices must be retrieved every 2-3 days. Upon retrieval, the adversaries will download any data and recharge the device before redeploying it. The two devices in the data set with wireless data capabilities both targeted point-of-sale terminals, where the device can be made physically larger. However, the adversaries do not have the capability to arbitrarily size their skimmers; the amount of space available is dependent on the targeted payment device.

For adversaries to successfully skim an ATM card (the most common attack in this dataset), they must also capture the victim's PIN. There are two mechanisms to accomplish this:

First, the adversary can deploy a camera to record the victim's hand as the PIN is typed. Figure 4 shows a frame of a real video from a skimming camera released to us by police. These cameras are most frequently fully-independent devices, containing their own storage and battery. The attacker relies on time sequences to manually match PIN entry video to card data. We observed that when law enforcement tries to determine if a payment device has a skimmer, they first look for the camera's pinhole since it is faster for them to identify than other mechanisms (e.g., deep-inserts, which we describe below), *further indicating that advice such as pulling the card acceptor may not be effective*. These cameras are small enough that adversaries can hide them inside ATM light fixtures. Figure 5 shows such a pinhole camera. Adversaries remove the light figures from ATMs, drill small holes, mount the cameras behind the lights, and remount the lights. Such a small hole is made more difficult to spot when a bright light shines near it; consumers cannot reasonably be expected to find these. We measured the camera pinhole on a skimmer (shown later in Figure 13c) at 1 mm. Accordingly, these devices are nearly impossible for consumers to visually detect, invalidating Tip 1.

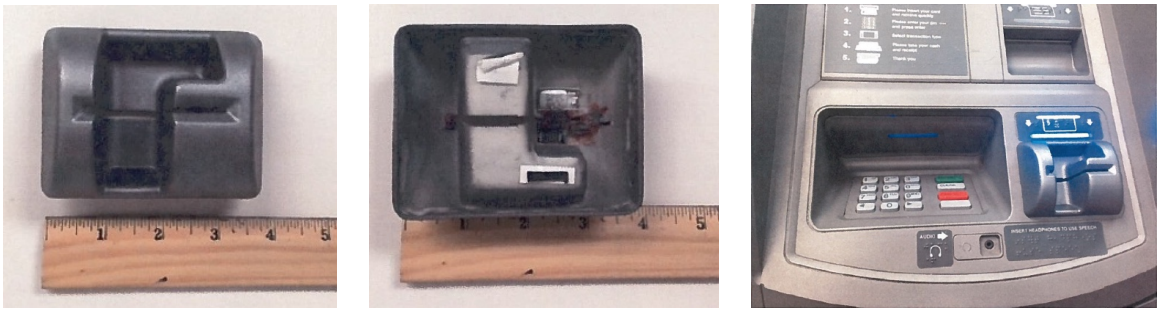
Second, the adversary can deploy a PIN pad overlay onto a point-of-sale terminal. These devices are placed on top of the original PIN pad such that when the victim enters their PIN, each press is received by both the overlay and the payment terminal. Such a device can be seen in Figures 6 and 13g. Ultimately, these devices are also difficult to detect because they are custom fit to the attacked terminal.

Deep-Inserts are placed inside the magnetic stripe card slot. These devices were constructed of a metal frame custom fit to the internals of the target machine. Figure 7 shows a deep insert skimmer recovered by the NYPD. To install these, adversaries use a tool to push the skimmer into the card slot and press it down. The skimmer sits in a small empty space inside the card acceptor, which can lead to a small amount of resistance between a victim's card and the skimmer as the card drags on the skimmer.

Like overlays, they contain an additional read head, decoding and storage hardware, and a small battery for performing an independent read of the card. They also must be removed for recharging and data retrieval.

Wiretaps sit on the communication path (typically an Ethernet cable) and perform a man-in-the-middle attack on the transmitted card data. The fact that this attack is effective implies that basic best practices for handling sensitive data (e.g., SSL/TLS with working certificate validation) are often not properly deployed.

EMV Shimmers are installed inside the EMV card slot and intercept the communication path between the EMV chip on the card and the payment terminal. Since the EMV chip contains a nearly-complete replica of the magnetic stripe data, acquiring this data has some value to the adversary. However, the chip does not contain the CVV1 present on the stripe; instead, it provides a code known as the iCVV. This prevents the adversary from making a perfect counterfeit magnetic stripe card, though



(a) Front (b) Rear (c) Installed

Figure 3: The front and rear of a typical overlay skimmer along with a photo of the skimmer installed on a real ATM, as captured by the NYPD. From the rear, the hardware for reading and storing the card data can be seen.

Figure 4: This is a frame of video captured by a camera deployed alongside a skimmer. The adversary uses the camera to capture the victim's PIN upon entry. With both card data and the PIN, the card can be used to obtain cash.

the cards may be used where CVV validation is not performed [33].

3.1.2 Internal-Access Skimmers

Internal skimmers are physical taps installed inside a payment terminal. They intercept the communications path between the card reader and other components. As a result, this single device provides access to both card data and any entered PIN.

This type of skimmer was found only inside gas pumps. These devices tap power from the host device, allowing permanent deployment with wireless data retrieval capabilities. As a result, all 5 of the recovered internal skimmers contain Bluetooth hardware for obtaining the data. Since there is no outward appearance of tampering, our contacts informed us that these often

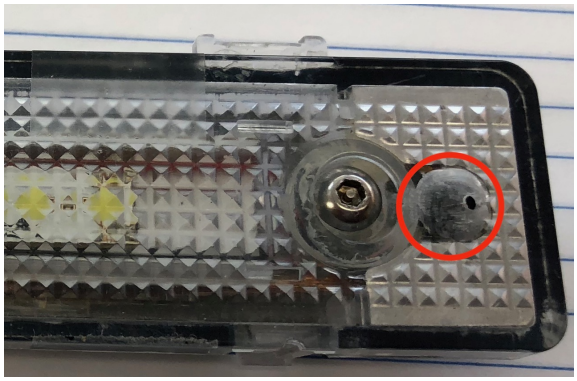


Figure 5: Adversaries modify original ATM light fixtures with pinholes for cameras, such as the one circled in red.

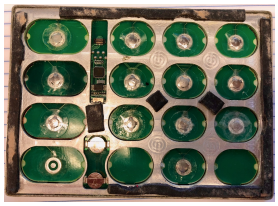
capture cards for months before detection.

3.2 Targets

Banks and ATMs represented the majority of targeted locations and devices. We initially believed that banks would have sufficient security measures to deter attackers. However, upon discussion with law enforcement officers, we found that these are targeted because their ATMs are often in the front where they can be accessed when the branch is closed. Furthermore, they are likely to offer attackers some privacy during off-peak times. Branch ATMs are kept behind locked doors when the branch is closed, allowing customers to swipe their card on the door for access to the ATMs. Door skimmers are functionally identical to other overlay deep-insert skimmers. As a result, the door locks are not only ineffective at restricting access from attackers, they are also a source of card data. Attackers with both card data and a PIN can recover large sums of cash in a short time. The ease of this attack leads ATMs to be the most targeted device with 74% of recovered skimmers.

Gas stations followed banks, which our contacts in-

(a) PIN Pad Overlay



(b) Reverse

Figure 6: PIN pad overlays can be applied over the payment terminal to collect the PIN as the victim enters it, allowing the adversary to use a skimmed card to retrieve cash from an ATM.

(a) Top

(b) Bottom

Figure 7: This deep-insert skimmer is machined to a custom fit for the targeted payment terminal.

formed us is due to poor security measures taken by these locations. The access to the payment device internals is protected by a simple lock. No alarm is triggered when the pump is opened, so adversaries that operate quickly and discreetly encounter no resistance to installing an internal skimmer inside the pump. Although it is often difficult to know the exact date the skimmer was installed, the NYPD told us that these skimmers can be in place as long as 6 months without detection. Unlike the majority of external skimmers, we believe this problem is caused solely by poor operational standards and could be resolved with basic physical security practices.

Finally, restaurants, hotels, and other retail establishments constitute the remaining 17 skimmers in the data set. ATMs remained the primary targeted device, however in these locations overlay skimmers were preferred over the deep-inserts seen at banks. The retail standalone ATMs typically found in these locations are manufactured by different vendors (e.g., Hyosung, Triton) than those installed at banks (e.g., Diebold, NCR). We suspect that the manufacturer and model may influence the type of skimmer used, but our dataset does not contain complete make and model data.

3.3 Data Retrieval and Bluetooth

Despite the prevalence of smartphone applications which claim to detect skimmers via Bluetooth, only 7 of 35 (20%) of the skimmers recovered by NYPD had wireless data retrieval capability; all were internal. Three BOLOs did not specify wired or wireless retrieval. No other skimmer, including the deep-inserts and any ATM skimmer, had this capability; they require the adversary to remove and connect the device to download the data. Accordingly, *existing detection technologies that rely on this feature cannot successfully detect the majority of skimmers* and Tip 3 is unlikely to protect users against most skimmers.

The majority of skimmers detected (71%) use serial, SPI, or I2C communication to download the data. During this time, the adversary can also recharge the device and choose a new location for deployment. Due to the small amount of physical space in most overlay and deep-insert skimmers, batteries must be small and hardware is limited to essential features. All of the internal skimmers discovered use wireless data retrieval, which is possible since these devices can be physically large and tap power from the host terminal.

3.4 Summary

The data from the NYPD Financial Crimes Task Force shows that the majority of skimming attacks are against ATMs and are performed using overlay and deep-insert skimmers, with are difficult to detect without expertise and tools. Since these devices must be small enough to fit on or in the card acceptor's slot, there is little room to deploy features such as a Bluetooth module. Adhesives used to affix overlays are strong enough to resist being pulled off, and deep-insert skimmers require special tools to remove. As a result, common advice on how to detect these devices is unlikely to produce a reliable result.

4 Designing a Skimmer Detector

With an understanding of the types and prevalence of skimmers, we now focus our attention to the problem of detecting skimmers. In this section, we state our hypothesis, define the common properties of skimmers, and implement the Skim Reaper, which uses these properties to prove the hypothesis.

4.1 Hypothesis

The most prevalent types of skimmers seen in the NYPD dataset are overlays and deep-inserts. These two types of devices both add a second read head to the card slot, such that when a card is legitimately read, an additional

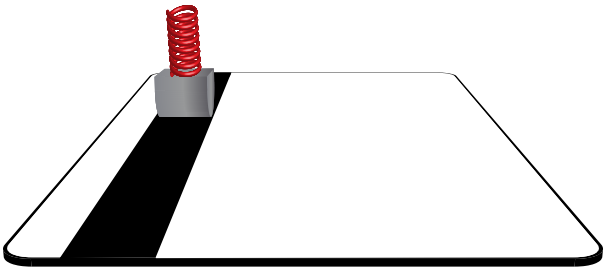


Figure 8: A spring mechanism pushes the card and head together to eliminate gaps, which lead to read failures.

read occurs by the skimmer. Using properties intrinsic to magnetic stripe reading, these read heads can be independently detected. The number of read heads detected can then be used to identify skimming attacks.

4.2 Fundamental Properties of Overlay and Deep-Insert Skimmers

Through examination of the NYPD's data set and a variety of magnetic stripe devices we acquired (e.g., dip- and swipe-style readers and card encoders), we identified three common characteristics of skimming technology:

1. **Touch:** In order for data to be accurately read from a magnetic stripe card, the magnetic read head must make physical contact with the card. Magnetic read heads are inductors; a voltage is produced in the presence of a changing magnetic field, which produces a current through the read head (or eddy current) [49]. This principle is outlined by Maxwell-Faraday's Law of Induction. From this law, a greater change in magnetic field intensity is directly correlated to the voltage and current generated in the magnetic read head.

   The magnetic field strength of a magnetic stripe card imposed on a read head is by default small, approximately 24 μT [26], and becomes even smaller as the distance between the card and read head increase. Magnetic field intensity is heavily affected by distance and falls off at a rate of approximately r^3, where r is the distance in meters [26]. For example, if the magnetic stripe card and the read head are separated by only 1 mm the magnetic field intensity of the card imposed on the read head is approximately 2.4×10^{-14} T, similar to that emitted by the human brain [13].

   Due to this decrease in field intensity, guidance from both commercial reader manufacturers [38] and parts sellers [3] explicitly mention the need to apply force between the card and the head (illustrated in Figure 8):

   > *"The most important part of aligning/placing the magnetic read head is ensuring that the magnetic read head is always completely flush against the magnetic stripe. This includes any curves or bends in the card. If [the] magnetic read head is not perfectly against the card at any point of the swipe, you will have a poor read."* [3]

   Without touching the card, the signal from the magnetic read head is unable to be accurately decoded.

2. **Surface Material:** On every read head we have observed, both in-person and via the NYPD dataset, the read head appeared to be metallic in (at least) those parts that are intended to be aligned with the card's data tracks. For the read head to function at the most fundamental level, the head must be a conductor. In order for the magnetic stripe card to induce an eddy current in the read head, the voltage induced must be significant. Constructing the track-aligned sections of the read head out of metal provides a low resistance, thus maximizing the voltage induced by the magnetic stripe. Due to this, the face of the read head must be a conductor.

   We verified on 17 different heads that this material is both metallic and electrically conductive.

3. **Size:** We observed a wide variety of sizes and shapes of read heads. Due to the limited space in overlay and deep-insert skimmers, adversaries produce and acquire smaller equipment. In the skimmers we observed, the smallest read head we encountered still contacted the card over a 1.5 mm section of the head. We attempted to find heads that contact the card over a smaller distance through skimmer sales channels, and found many heads that are thinner (i.e., low profile, 0.5 mm). These low-profile heads also make 1.5 mm of contact.

   As a result, we believe that the smallest available heads still make over 1 mm of contact, and that reducing the size further is either cost prohibitive or physically impossible while retaining accurate card reading.

These three properties constitute fundamental aspects of card reading; that is, we believe that adversaries seeking to read cards reliably must adhere to designs which meet these characteristics.

4.3 Implementation

We now discuss our prototype implementation of detection mechanisms for the above properties, called the

Figure 9: This is the entire Skim Reader device, consisting of the microcontroller system (left) and the measurement card (right). The card is inserted into a card acceptor, where the number of read heads is measured by the microcontroller. After the user indicates that the test is complete, the user is notified if a skimmer was detected.

Figure 10: On the measurement card, a pattern of traces pass over read heads for detection. The black lines on the left indicate the pattern and position of the traces, which are aligned to the expected data track locations (shown on right for comparison). When a read head passes over the card, the traces are bridged and a circuit is completed. The traces are separated by 0.1 mm of space, which is over an order of magnitude smaller than the smallest read head we encountered.

Skim Reaper. The device, shown in Figure 9, consists of a payment card-sized board and a microcontroller system, which provides 3.3 V to the card and performs analysis. The card is intended to be inserted into the card acceptor on a payment device, and relies on the properties of magnetic read heads discussed above to improve detection and increase the difficulty in developing effective countermeasures.

As we previously discussed, the skimmers identified in our NYPD data set are designed to press a metallic read head against the card during capture. Our system relies on these two properties and expects read heads in the card acceptor to contact our card and bridge a pair of electrical traces, which complete a circuit back to the microcontroller. To ensure correct alignment, the card is the height and thickness of a standard payment card. On this card, we placed a series of split copper interconnections aligned with the ISO-standard locations [29, 30] for the three card tracks, as shown in Figure 10. This design ensures that if a skimmer is aligned to read a particular

(a) Sankyo Reader

(b) with Custom Skimmer

Figure 11: We used a Sankyo MCM2PO stripe reader and a custom 3D-printed skimmer to verify the effectiveness of the Skim Reaper.

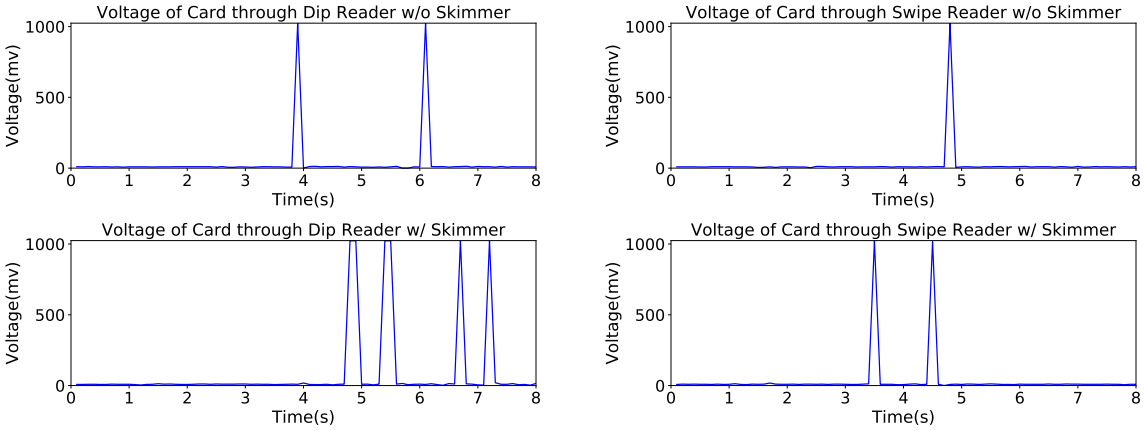
card track, it will also pass over our traces.

The distance between each trace is 0.1 mm, which is over an order of magnitude smaller than the shortest track read length we observed (1.5 mm). As a result, these read heads will bridge the traces, complete the circuit, and be counted. We mirrored the traces on the card and placed the wires to the top of one side; this allows the card to successfully contact read heads in any configuration of both dip- and swipe-style readers.

During early prototyping, we encountered problems creating PCB masks that met our 0.1 mm needs; this level of precision is difficult to obtain by hand. We overcame this by spray painting bare copper-clad board then used a laser cutter to vaporize the areas not covered by the mask. We then chemically etched the board and removed the leftover spray paint with acetone. This is a time-consuming, manual process with each card taking several hours to finish. As our design choices became finalized, we encountered a different problem with this method: the chemical bath would occasionally dissolve the copper underneath the spray paint, leading to a high manufacturing failure rate. We produced our final prototype device using PCBs produced in a professional fabrication facility based on our circuit diagrams.

The analysis device consists of an Adafruit [1] Arduino based microcontroller which applies voltage to one half of the traces and monitors for circuit completion on the opposite half. To prevent noise in the signal from causing false positives, the device samples the card, averages every 20 samples to counter the effects of having an imperfect ground, and compares it to a threshold. If the value is above the threshold, one is added to the current read head count. The microcontroller waits for the average voltage to drop back below the threshold, which indicates that the read head has fully passed over the card. After this the microcontroller begins again looking for an average voltage above the threshold. This repeats until the user indicates that the test is complete.

When counting the read heads in a card acceptor, the count can vary depending on the type of reader. For example, in a swipe-style reader, each read head passes



(a) Dip Mode

(b) Swipe Mode

Figure 12: As the Skim Reaper passes over read heads, the microcontroller measures the voltage returned from the measurement card, shown above. The voltage spike indicates that a read head was encountered as a circuit is completed using the head. In dip mode, the device internally halves the count because each head passes over the card twice (once on insert and once on removal). We used the Sankyo MCM2PO reader with our custom skimmer for confirmation testing in dip mode, and we used a standard stripe reader (1 head) and a stripe encoder (2 heads) for testing in swipe mode.

over the card only once. In dip-style readers, however, each head will pass the card twice: once on insert and once on removal. Due to this use case, our device has a switch to allow the user to identify the type of reader being examined.

Finally, the Skim Reaper uses this count to alert the user to the presence of skimmers. If more than one read head is detected, the user is alerted. If one read head is detected, a notification appears that the reader appears to be normal. In other conditions (including zero heads detected), an error is displayed.

5 Confirmation and Analysis

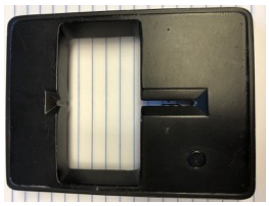
We now describe our experimental evaluations of the Skim Reaper and show that our system is effective in detecting overlay and deep-insert skimmers.

5.1 Confirmation

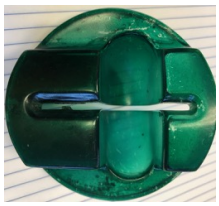
During our initial design, we needed to quickly test prototype iterations. Skimmers are difficult and expensive to obtain; "retail" prices for overlays can reach hundreds of dollars for the bezel alone (without electronics or read heads, which can easily triple the price of a complete unit) [2]. Many skimmer sellers require the customer to wire funds with no guarantee of receiving the item. Furthermore, it is unclear whether these businesses are legitimate or if the funds are used for criminal purposes. To avoid needing to purchase a skimmer, we first designed and built a skimmer suitable for testing.

We purchased a Sankyo MCM2PO reader and designed and 3D-printed a conspicuous, brightly-colored overlay skimmer for it, shown in Figure 11. The Sankyo device is an OEM replacement part for a gas pump payment terminal. Our overlay extends the card track from the original card reader, holding a standard Square Reader in the track. Since our detector detects the presence of the read head, the Square Reader does not need to be further connected to any device (e.g., for decoding).

Testing the Skim Reaper with this skimmer is the same process as detecting any other skimmer: We select the dip mode on the device, enable detection, insert the card into the card track, then remove it. We performed this task with and without the skimmer attached to verify that our system correctly identifies its presence. Figure 12 shows our device as it encounters heads. As the card passes over read heads, the circuit completes, creating a voltage spike. Since the card passes over each read head multiple times in dip mode (once on insert and once on removal), the number of spikes seen is double the number of heads.



(a) ATM Overlay



(b) ATM Overlay

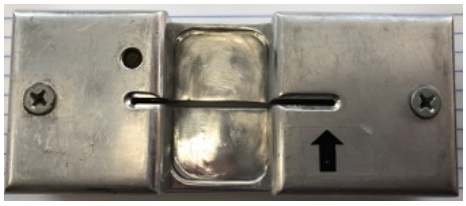
(c) ATM Overlay

(d) ATM Overlay

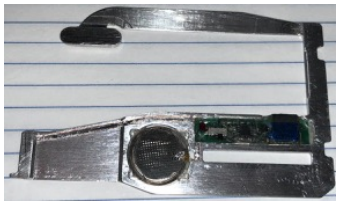
(e) ATM Overlay

(f) ATM Overlay

(g) POS Overlay



(h) ATM Door Access Overlay



(i) Deep-Insert

(j) Deep-Insert

Figure 13: This figure shows the 10 real skimmers provided to us from the NYPD. The Skim Reaper successfully detected all of these skimmers.

5.2 NYPD Evidence Set

While our testing with commercially-available read heads was successful, we observed that the readers examined in Section 3 had much smaller heads. We again partnered with the NYPD Financial Crimes Task Force to obtain skimmers from evidence storage[4]. In total, we obtained access to ten external-access skimmers consisting of eight overlays and two deep-inserts. Each of these skimmers is shown in Figure 13. Many of these skimmers were confiscated in campaigns identified by the BOLOs we discussed in Section 3. As a result, these skimmers represent a realistic subset of the skimmers found in New York City. We had no access to these skimmers prior to building our prototype Skim Reaper device.

Except for a single deep-insert skimmer, we also did not have access to the payment devices the skimmers were designed to attack. For the remainder of the devices, we used a modified protocol: Since the detection alert is based on the number of detected read heads, we can verify that our system will detect a skimmer by observing whether it detects a single read head when inserted into only the skimmer. We tested the Skim Reaper against each of these skimmers five times and recorded whether or not it successfully detected the skimmer. The Skim Reaper successfully detected the skimmers in all five attempts on all of the skimmers.

The deep-insert skimmer we were provided with its payment terminal did not contain an additional read head like others we have observed. Instead, it appeared to use thin 30 AWG solid-core bare copper wires bent upwards, away from the skimmer, to physically tap the existing magnetic read head. We discovered this mechanism after our system successfully detected the skimmer and we removed the skimmer from the payment device. We disassembled the payment device to learn more about this mechanism and discovered that the flexible flat ribbon cable used to connect the read head to the body of the payment device was not coated. As a result, the cable provided an exposed electrical connection to the read head. Unfortunately, we were not able to determine whether this device worked since removing it from the skimmer damaged the tap mechanism. We believe this is a hardware vulnerability stemming from the lack of coating on the cable, though successfully executing this attack requires the attacker to have some luck to accurately place thin copper wires onto thin copper traces on the ribbon cable without visibility. Regardless, our system detected the deep-insert since the body of the skimmer was metal and still contacted the measurement card.

[4]The skimmers were from closed cases.

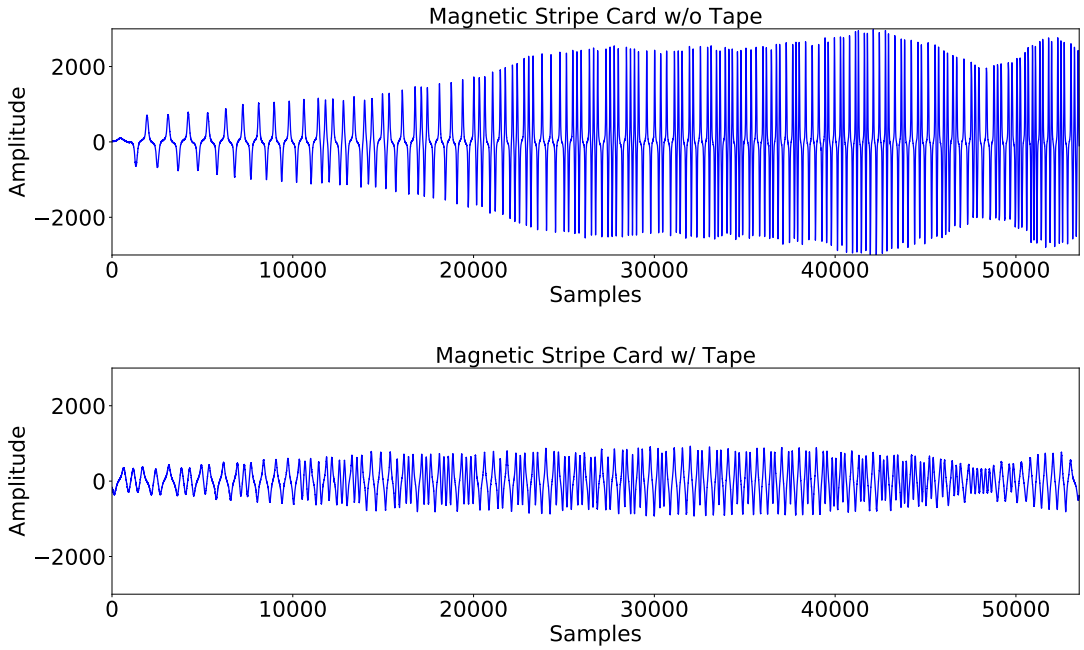


Figure 14: We recorded the raw magnetic signal from a skimmer's head with and without tape attached to it. Tape could be used to reduce the conductivity of the head as a countermeasure, but this ultimately fails as the signal is reduced to the point of being unreadable.

5.3 Ongoing Detection

The Skim Reaper successfully detects every overlay and deep-insert skimmer we have obtained, and as we have shown, making these undetectable relies on overcoming current limitations in reading magnetic stripes, confirming our hypothesis. Using the properties of skimming technology, our system provides a substantial benefit to consumers and law enforcement officers who wish to identify the presence of skimmers earlier.

The NYPD Financial Crimes Task Force requested a set of Skim Reaper devices for use in the field, which we provided. These devices are now being used by detectives in the field to proactively identify skimmers or verify skimmers are present when investigating a complaint.

6 Countermeasures and Discussion

During the course of testing the Skim Reaper, we had the opportunity to closely observe skimmer technology. In this section, we discuss adversarial countermeasures to detection and outline additional information about these devices.

Reducing conductivity: One seemingly obvious way to avoid detection is to make the head non-conductive. We addressed the requirement for the head to be conductive in Section 4.2, however applying tape or laminate to the head may also reduce the conductivity to the card without modifying the head. Such an addition does not change the construction of the head, but both create a gap between the head and stripe and eliminate the conductivity of the card/head interaction. In fact, applying tape to the magnetic stripe is a common fix for read errors on worn cards [23]. However, this fix works because the read heads typically found in point-of-sale terminals and other commercial applications are physically larger than those found in skimmers, a property that makes them more sensitive to the weaker signal produced by a magstripe through tape.

To verify, we tested this on the skimmer shown in Figure 13c. We recorded the raw signal produced by the skimmer's read head at a 96 kHz sample rate while we swiped a card with and without tape, shown in Figure 14. With tape, the recorded signal is diminished and unreadable. We attempted 50 times to read the card and decode its data through tape, but were unsuccessful. Accordingly, taping the read heads is not a viable option for avoiding detection.

Other commonalities: Each of the overlay and deep-

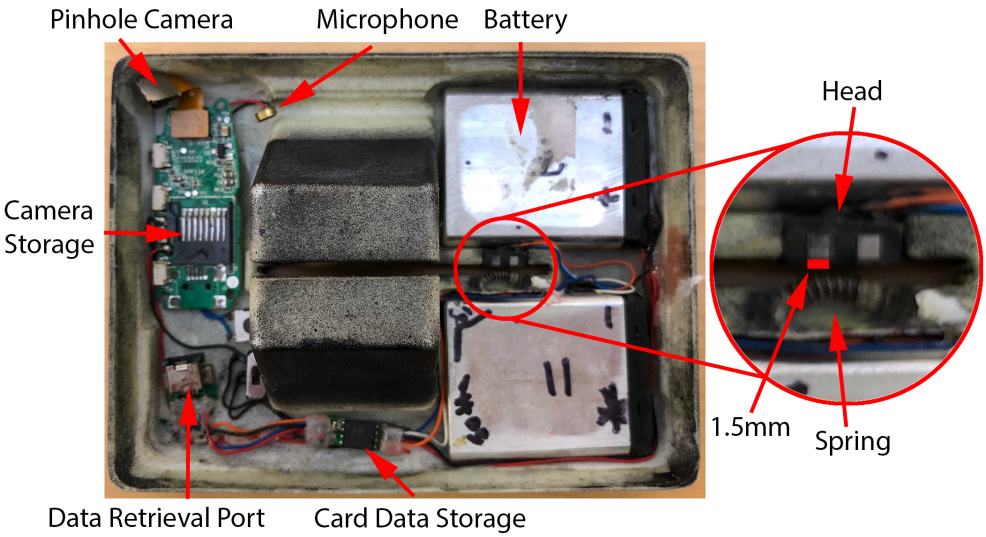


Figure 15: This is the reverse side of the skimmer shown in Figure 13c. The head and spring mechanism are enlarged, and the track-aligned conductive portion of the head is visible; we measured this at 1.5 mm. The pinhole for the camera is obscured by the camera housing, however we measured the pinhole at 1 mm.

access skimmers we examined is functionally identical. Internally, each device contains a microcontroller that receives a signal from a magnetic read head. The card data is then stored on a flash memory IC that is communicated with via exposed female headers. We were unable to identify the ICs used in each skimmer because the information on the surface of the chips (e.g., model information) is filed or etched off. The internals of one of the skimmers pictured in Figure 13 can be seen in Figure 15

All of these devices were powered by lithium-ion batteries. Some are easily rechargeable via female headers, while others provide no charging mechanism. The main variation in batteries is size and capacity, which we found typically fit exactly the available space after installing the other components. Several skimmers we examined contained multiple batteries connected in parallel, which is poor practice because it can cause the batteries to be unstable, and thus creating a fire hazard.

Ultimately, these devices differ only in their form factors.

7 Related Work

Electronic payment systems are vulnerable to a variety of attacks. These attacks include transaction snooping [43, 40], fraudulent accounts [25, 19], counterfeit/tampered transactions [42, 46], and double spending [18, 31]. The most widely deployed electronic payment system, the magnetic stripe card, does not offer any security features, making them trivial to attack and duplicate [7]. Data stolen from magnetic stripe cards can be sold online or be used to fabricate counterfeit cards that can then be used in physical stores [10, 6]. One of the primary methods of attacking magnetic stripe cards is through skimming devices, more commonly known as "skimmers" [36].

Attempts have been made to increase the security of magnetic stripe cards through examining account transactions and identifying fraudulent activity. Some of the methods of detecting illegitimate transactions incorporate data mining and machine learning to profile these transactions based on historical data [16, 51, 17]. Using the Hidden Markov Model [50] and profiling normal card behavior [8, 9] have also been proposed. These methods are a "best guess" effort and do not always prevent malicious transactions. The results of these methods are similar to current practices by credit card companies to identify the use of stolen magnetic stripe card data. Efforts have also been made to authenticate magnetic stripe cards via physical characteristics of the data encoded on the cards. MagnePrint [4] attempts to resolve this problem by authenticating the physical magnetic material. The system calculates a fingerprint using the noise present between peaks in the analog waveform and matches it to a known value. Major faults of MagnePrint is that it requires the card to be measured at the time of manufacture and it requires the merchant to transmit the calculated signature during the authorization process. More recently an improved system was developed that detects fraudulent magnetic stripe cards, without the need to measure magnetic stripe cards at the time of manufacture [48].

EMV, widely known as Chip-and-PIN, are tamper resistant cards that run code to perform card authentication with the issuer. Though EMV provides more security features than magnetic stripe cards, EMV cards are still susceptible to a variety of attacks [53, 37, 12, 20, 22, 41, 21, 15]. Skimming devices specifically designed for EMV cards also exist [33, 14], known as Chip-and-Shim devices. In addition to attacks EMV has also experienced deployment issues [24, 39]. While EMV is a more secure alternative to magnetic stripe cards, these cards will not replace magnetic stripe cards any time soon [27], demonstrating that magnetic stripe card fraud will continue to be a prevalent problem that our system addresses.

8 Conclusion

Skimmers represent a significant and growing threat to payment terminals around the world. Moreover, adversaries have become increasingly sophisticated, making the detection of such attacks difficult. We address these problems by conducting the first large-scale academic analysis of skimming devices. With a characterization of the techniques *actually* being used by attackers, we first debunk much of the common advice offered to protect consumers. We then develop the Skim Reaper tool, which relies on the necessary physical properties of the most common types of skimming devices found in New York City. After successfully testing our solution on skimmers used in real crimes, we show that simple adversarial countermeasures are ineffective against our device. Accordingly, though systematization, characterization and measurement, we show that robust and portable tools can be developed to help consumers and law enforcement to rapidly detect such attacks.

Acknowledgments

The authors would like to thank the NYPD Financial Crimes Task Force for their invaluable assistance with this work.

References

[1] Adafruit industries. https://www.adafruit.com/.

[2] DB001 ATM bezel overlay designed by MSR Tron. https://web.archive.org/web/20180205133533/http://msrtron.com/atm-bezels/db001. Archived: 2018-02-05 at the Internet Archive.

[3] Magnetic read head alignment guide. http://msrtron.com/blog-headlines/read-head-alighment.

[4] Welcome to MagnePrint®: What is MagnePrint? http://www.magneprint.com/, 2016.

[5] The Nilson Report. https://nilsonreport.com/upload/content_promo/The_Nilson_Report_Issue_1118.pdf, Oct. 2017.

[6] ABC NEWS. Why chip credit cards are still not safe from fraud. YouTube - https://www.youtube.com/watch?v=gJo9PfsplsY, 2016.

[7] ACCPACONNECTION. Credit card skimming operation. YouTube - https://www.youtube.com/watch?v=U0w_ktMotlo, 2008.

[8] AGRAWAL, A., KUMAR, S., AND MISHRA, A. Credit card fraud detection: A case study. In *2nd International Confrence on Computing for Sustainable Global Development (INDIACom)* (2015).

[9] AGRAWAL, A., KUMAR, S., AND MISHRA, A. A novel approach for credit card fraud detection. In *2nd International Confrence on Computing for Sustainable Global Development (INDIACom)* (2015).

[10] AMERICAN UNDERWORLD. Report on carding, skimming. YouTube - https://www.youtube.com/watch?v=k_brU9Jwhww, 2012.

[11] ANDERSON, R. Why Cryptosystems Fail. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)* (1993).

[12] ANDERSON, R., AND MURDOCH, S. J. EMV: Why payment systems fail. *Communications of the ACM 57*, 6 (2014).

[13] BARANGA, A. B. Brain's magnetic field: a narrow window to brain's activity. In *Electromagnetic field and the human body workshop* (2010).

[14] BOND, M., CHOUDARY, O., MURDOCH, S. J., SKOROBOGATOV, S., AND ANDERSON, R. Chip and skim: Cloning EMV cards with the pre-play attack. In *2014 IEEE Symposium on Security and Privacy (S&P)* (2014).

[15] BUKHARI, J. That chip on your credit card isn't stopping fraud after all. Fortune - http://fortune.com/2017/02/01/credit-card-chips-fraud/, 2017.

[16] CHAN, P. K., FAN, W., PRODROMIDIS, A. L., AND STOLFO, S. J. Distributed data mining in credit card fraud detection. In *IEEE Intelligent Systems and Their Applications* (1999).

[17] CHAN, P. K., AND STOLFO, S. J. Toward scalable learning with non-uniform class and cost distributions: A case study in credit card fraud detection. In *International Conference on Knowledge Discovery and Data Mining* (1998).

[18] CHAUM, D. Achieving electronic privacy. *Scientific American* (1992).

[19] CORKERY, M. Wells fargo fined $185 million for fraudulently opening accounts. The New York Times - http://www.nytimes.com/2016/09/09/business/dealbook/wells-fargo-fined-for-years-of-harm-to-customers.html, 2016.

[20] DE RUITER, J., AND POLL, E. Formal analysis of the EMV protocol suite. In *Theory of Security and Applications* (2011), S. Mödersheim and C. Palamidessi, Eds., Lecture Notes in Computer Science, Springer Berlin Heidelberg.

[21] DRIMER, S., AND MURDOCH, S. J. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. In *USENIX Security* (2007), vol. 2007, pp. 87–102.

[22] DRIMER, S., AND MURDOCH, S. J. Chip & PIN (EMV) relay attacks. https://www.cl.cam.ac.uk/research/security/banking/relay/, 2013.

[23] DUTTON, J. Wired's Lab-Tested, Muppet-Vetted formulas for smartifying your life: Fix a credit card that won't swipe. *Wired* (Nov. 2011).

[24] HAMBLEN, M. Chip card payment confusion, anger rages on - Merchants blame card companies for delays in certifying EMV software. Computerworld - http://www.computerworld.

com/article/3059379/mobile-payments/chip-card-payment-confusion-anger-rages-on.html, 2016.

[25] HARRELL, E. Victims of identity theft, 2014. http://www.bjs.gov/content/pub/pdf/vit14.pdf, 2015.

[26] HAYT, W. H., AND BUCK, J. A. *Engineering Electromagnetics*, 7th ed. 2005.

[27] HOLMES, T. E. Payment Method Statistics. Creditcards.com - http://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php, 2015.

[28] HORAN, T. J. Double-Digit ATM compromise growth continues in US. http://www.fico.com/en/blogs/fraud-security/double-digit-atm-compromise-growth-continues-in-us/, Aug. 2017. Accessed: 2018-2-6.

[29] ISO. Identification cards - recording technique - magnetic stripe - low coercivity. 7811-2:2014(E), 2014.

[30] ISO/IEC. Identification cards - recording technique - magnetic stripe - high coercivity. 7811-6:2014/(E), 2014.

[31] KARAME, G. O., ANDROULAKI, E., AND CAPKUN, S. Double-spending fast payments in bitcoin. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)* (2012).

[32] KOHNO, T., STUBBLEFIELD, A., RUBIN, A. D., AND WALLACH, D. Analysis of an Electronic Voting System. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)* (2004).

[33] KREBS, B. Chip card ATM 'shimmer' found in Mexico. https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/, Aug. 2015. Accessed: 2018-1-29.

[34] KREBS, B. A Dramatic Rise in ATM Skimming Attacks. https://krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/, 2016.

[35] KREBS, B. All about fraud: How crooks get the CVV. http://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/, 2016.

[36] KREBS, B. All about skimmers. https://krebsonsecurity.com/all-about-skimmers/, July 2016. Accessed: 2018-1-29.

[37] LUCA, D., AND NOCERA, J. It's time to invest in EMV payment card systems. http://usblogs.pwc.com/cybersecurity/its-time-to-invest-in-emv-payment-card-systems/, 2014.

[38] MAGTEK. Magnetic card reader design kit. https://www.magtek.com/content/documentationfiles/d99821002.pdf, May 2017.

[39] MCQUAY, S. Why You Might Not See an EMV-Ready Gas Pump for a While. https://www.nerdwallet.com/blog/credit-cards/emvready-gas-pump/, 2015.

[40] MEIKLEJOHN, S. If privacy matters, cash is still king. *The New York Times* (2013). http://www.nytimes.com/roomfordebate/2013/12/09/the-end-of-cash/if-privacy-matters-cash-is-still-king.

[41] MURDOCH, S. J., DRIMER, S., ANDERSON, R., AND BOND, M. Chip and PIN is broken. In *2010 IEEE Symposium on Security and Privacy (S&P)* (2010).

[42] NEAL, D. J. A fraud factory in a small apartment made 1,000 fake credit cards a day, feds say. Miami Herald - http://www.miamiherald.com/news/local/community/miami-dade/hialeah/article186649473.html, 2017.

[43] NICOL, N. J. No expectation of privacy in bank records - United States v. Miller. *26 DePaul L. Rev. 146* (1976).

[44] NORTHRUP, L. The ATM Liability Shift Is Here, And Most Dont Have Chip Readers. https://consumerist.com/2016/10/21/the-atm-liability-shift-is-here-and-most-dont-have-chip-readers/, 2016.

[45] PAUL, N., AND TANENBAUM, A. S. The Design of a Trustworthy Voting System. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)* (2009).

[46] RHODEN, R. 4 men accused of spending spree with counterfeit credit cards. New Orleans Times - http://www.nola.com/crime/index.ssf/2017/02/4_men_accused_of_spending_spre.html, 2017.

[47] SANDLER, D., DERR, K., AND WALLACH, D. S. VoteBox: a tamper-evident, verifiable electronic voting system. In *Proceedings of the USENIX Security Symposium (SECURITY)* (2008).

[48] SCAIFE, N., PEETERS, C., VELEZ, C., ZHAO, H., TRAYNOR, P., AND ARNOLD, D. The cards aren't alright: Detecting counterfeit gift cards using encoding jitter. In *2018 IEEE Symposium on Security and Privacy (S&P)* (2018).

[49] SERWAY, R. A. *Physics for Scientists and Engineers*, 8th ed. 2009.

[50] SRIVASTAVA, A., KUNDU, A., SURAL, S., AND MAJUMDAR, A. Credit card fraud detection using hidden markov model. In *IEEE Trans. Dependable Security Comput.* (2008).

[51] STOLFO, S., FAN, D. W., LEE, W., PRODROMIDIS, A., AND CHAN, P. Credit card fraud detection using meta-learning: Issues and initial results. In *AAAI-97 Workshop on Fraud Detection and Risk Management* (1997).

[52] TOTAL SYSTEM SERVICES (TSYS), INC. 2016 U.S. Consumer Payment Study. https://www.tsys.com/Assets/TSYS/downloads/rs_2016-us-consumer-payment-study.pdf, 2016.

[53] URIARTE, C. Gift Card Fraud Will Be a Major Threat Post-EMV. https://www.paymentssource.com/opinion/gift-card-fraud-will-be-a-major-threat-post-emv, 2015.

[54] WILLIBY, H. Raw video: Men place card skimmer on ATM store machine! YouTube - https://www.youtube.com/watch?v=y83ZgzuFBSE&t=13s, Mar. 2016.