Please Pay Inside: Evaluating Bluetooth-based Detection of Gas Pump Skimmers

Abstract

Gas pump skimming is one of the most prominent forms of payment card skimming attacks today, but it is also one of the most difficult to detect. Skimmers are easily installed internally in gas pumps, evading all physical detection, and criminals can wireless exfiltrate card data with Bluetooth. Fraud from skimming is so significant that officials in Arizona to routinely inspect every PoS terminal (i.e., fuel dispenser) for these skimmers, requiring dedicated teams of inspectors.

In this work, we present the results of our large-scale study of the effectiveness of detecting gas pump skimmers faster with Bluetooth. During the course of the study, we collected Bluetooth scans at 780 gas stations in six states, where we detected a total of 37 skimmers across four U.S. states, all of which were recovered by law enforcement. We discovered that skimmers are clearly distinguished from legitimate devices in Bluetooth scans at gas stations. We also found several surprising aspects of the nature of gas station skimming: skimmers can be installed in gas pumps for months without detection, MAC addresses of skimmers are similar across geographic areas.

1 Introduction

Payment card skimming attacks at gas pumps have reached alarming levels. In 2018, law enforcement captured 972 skimmers from gas pumps in Florida [8], 148 skimmers in Arizona [32], and 42 just in San Diego County\(^1\). We estimate that criminals make $15,000 per day from each skimmer\(^2\) (Section 2.2). Therefore, these skimmers may have lead to a total of $22.5 million in fraud each day that they were in operation. In one instance, a skimmer gang was indicted after committing $2.1 million in card fraud with a deployment of gas pump skimmers in Texas, Georgia, and South Carolina [2].

Compared to other skimming targets (e.g., ATMs and retail Point-of-Sale terminals), gas pumps are an ideal skimming target. Gas pumps have relatively weak security: their payment circuitry can be accessed with universal keys or crowbars, and reading payment data is as easy as tapping into a ribbon cable (Section 2.1). They are also difficult to detect: the skimmer circuit is hidden inside the gas pump, and it is equipped with a Bluetooth transmitter, so criminals can wirelessly exfiltrate the skimmed card data from a safe distance [20, 21, 22, 23]. As a result, the most common way for law enforcement to detect if a gas pump has a skimmer installed, is to open the pump and inspect the wiring for a skimmer.\(^3\) Routine inspections of gas pumps are now common in many jurisdictions. For instance, public inspection reports from the Arizona Department of Weights and Measures reveals that in 2018, their personnel performed 1,311 gas station inspections for skimmers. Skimmers however were rarely found; inspectors only found skimmers in 3.4% of their inspections.

While Bluetooth is a vital tool for criminals to exfiltrate data from gas pumps, it also could be a weakness that makes it easier to detect if a pump is being skimmed. Indeed, if a skimmer can be detected automatically with a low-cost Bluetooth scanning tool (e.g., a smartphone), then authorities can discover and remove some of the skimmers passively and quickly while they visit a gas station for other reasons.

In this paper, we evaluate the effectiveness of detecting skimmers with simple Bluetooth scans. We developed an application that collects all Bluetooth scan data available via the standard Android API—including information that has not been considered in the few Bluetooth skimmer detection tools that are available for consumers [3, 38, 5]. We equipped 44 volunteers in six U.S. states with smartphones running this scanning tool. They scanned a total of 780 gas stations for Bluetooth devices, and observed 1,590 Bluetooth devices. From these scans, we detected 37 skimmers installed gas stations in Arizona, California, Nevada, and

\(^1\)Source: A federal law enforcement agency.

\(^2\)$500 per card, and skimmers tend to capture 30 cards per day.

\(^3\)These inspections are infrequently triggered by complaints.
Maryland. Immediately after we detected each skimmer we informed law enforcement, and they removed the skimmers and collected them as evidence. We estimate that the removal of skimmers we found during this study stopped a total of $555,000 in fraud per day they were operating.

With this scan data, and the knowledge of how skimmers appear in Bluetooth scans, we performed an empirical study to measure how effective scanning for the Bluetooth signals from skimmers is today; and how effective it will be in the future. The key result of the study is the observation that it is feasible to differentiate skimmers from other common Bluetooth devices that are found at gas stations. We found that signal strength is a reliable way to determine if a Bluetooth device is located near a gas pump, and thus is a suspected skimmer, even if it does not match the characteristics of typical skimmers. We also found that the Bluetooth Class-of-Device—a parameter not collected by any of the Bluetooth scanning applications—is the same for all of the skimmers we recovered; therefore, it is an excellent way to filter out legitimate devices.

We also discovered there are issues with consumer applications that detect skimmers with Bluetooth scans that can be improved: there are many legitimate products that appear at gas stations that use the same Bluetooth modules a skimmers, therefore MAC address-prefix based detection used in several applications is unreliable. Also, there are many Bluetooth modules that do not comply with IEEE MAC assignment requirements; they assign the addresses in a way that we can detect if it is likely to be a skimmer. We also debunk popular advice from authorities: “When you are standing near a pump... if you see a long string of numbers trying to connect with your phone, that is a sign of a nearby skimmer” [5]. We also inadvertently ran a natural experiment where we observed that skimmers had been installed in gas pumps for up to six months without detection.

Performing this in-depth study brought to light several important operational lessons learned about the importance of detecting skimmers with Bluetooth for improving skimmer inspections. Using Bluetooth scans, officials often detected skimmers while driving by gas stations that they otherwise would not have inspected. We also witnessed several instances where an inspector could not find a skimmer on their first pass looking inside a gas pump; however, they persisted and found it based on the knowledge that a suspected skimmer appeared to be in the pump based on Bluetooth scans. Surprisingly, we discovered that skimmers installed in the same gas station, or city, often have very similar MAC addresses, indicating their source is a single criminal entity. We even found skimmers installed hundreds of miles away that had surprisingly close MAC addresses.

The rest of the paper is organized as follows: Section 2 provides background on internal gas pump skimming: their construction, monetary incentive, and prevalence in the wild. Section 3 is an overview of the data collection methodology we used for the measurement study and a description of Bluetana. In Section 4 we present the results of our study: both describing how skimmers look like and whether they are well hidden in the environment. In Section 5, we present possible counter measures to the Bluetooth detection. In Section 6 we present the operational lessons we learned about skimming and criminal investigation procedure, while performing our large scale measurement study. Section 7 is related work, and we conclude in Section 8.

2 Background

Skimmers are illicit devices that capture credit card magnetic stripe data when a card is used at a point-of-sale (PoS) terminal or automatic teller machine (ATM). Traditional skimmers use a magnetic head concealed in a false faceplate to read the magnetic stripe of a card as it is inserted into the real card reader. This paper is concerned with a new class of skimmers, which we term internal skimmers, that are installed entirely inside a PoS terminal or ATM, leaving no visual evidence of its presence. Internal skimmers attach to the cable that connects the card reader to the main circuit board of the PoS terminal, tapping the data lines and drawing power from the cable.

To make data collection easier, many internal skimmers include a Bluetooth-to-serial module that allows the perpetrator to collect the “skimmed” data without having to physically accessing the internal skimmers. Fuel pumps with a built-in PoS terminal have become a very popular target for such internal skimmers: they are unattended, easy to access, and have poor physical security, which make it easy to install a skimmer without being noticed. In a typical installation scenario, an attacker positions a van at a fuel station to block the station attendant’s view of the target pump, opens the fuel pump using a common master key, and clips a discreet gumstick-sized skimmer to the ribbon cable between reader and main circuit board using a vampire clip. The entire process to install skimmer can take less than 10 seconds [1]. The perpetrator can then return to the same station with a laptop or smartphone, connect to the skimmer using Bluetooth, collect the “skimmed” data, and leave without leaving the vehicle. The subject of our investigation is these internal, Bluetooth-based skimmers that are installed in fuel pump PoS terminals. These skimmers are built using commodity hardware with a total unit cost of $20 or less, as described next.

2.1 Internal Bluetooth Skimmers

Figure 1 shows a typical Bluetooth skimmer, recovered from a fuel station in San Juan Capistrano, California. This skimmer consists of a Teensy development board with a 120 MHz ARM Cortex-M4F micro-controller and a Roving Networks RN-41 Bluetooth-to-serial module, along with ribbon cables,
headers, and cable clips for attaching to the ribbon cables inside the pump.

Connections. In the figure, the ribbon cable on the left connects to the ribbon cable that connects the magnetic stripe reader to the PoS terminal main board. The skimmer also uses this connect for power: the power and ground pins of the Teensy (on far left of board, not visible in Figure 1) are connected to power and ground on the magnetic stripe reader cable. The ribbon cable on the right connects to the ribbon cable from the PoS keypad. This allows the perpetrator to capture additional card verification data, namely the debit card PIN or credit card billing ZIP Code. Availability of a PIN code with a stolen debit card in particular, can increase its value five-fold on the black market (Table 1). However, not all skimmers capture keypad data.

Most gas station skimmers read the unencrypted data pulled from magnetic stripe readers. Card issuers feel that removing sensitive data from the magnetic strip on cards will help to solve the problem [35]. Newer literature has demonstrated attacks on chip payment systems [11, 12], and law enforcement in Latin America have begun to find EMV skimmers that are Bluetooth enabled [24, 4].

Controller board. The skimmer pictured in Figure 1 used a Teensy micro-controller development board equipped with a 120 MHz ARM Cortex-M4F micro-controller made by Freescale Semiconductor. By using a development board, a skimmer requires only rudimentary electronic assembly: soldering wires to the development board.

However, skimmers have also been found using what appeared to be fully custom-designed boards. These are compact, making them better for hiding in the dispenser. Examples of micro-controllers used in recovered skimmers include Microchip PIC18F4550 [3] and Atmel XMEGA128A4U [4].

Storage. The Teensy board also has a microSD card slot for additional data storage. Skimmers built on custom PCBs have also used flash and EEPROM ICs for storage. The storage capacities vary across designs, with examples including PCT25VF032B (32-M-bit) [4] and Micron M25P16VP (16-M-bit) [3].

Bluetooth module. The skimmer shown in Figure 1 uses a Roving Networks RN-41 module, an inexpensive Bluetooth-to-serial module found in many skimmers. In Section 4.2 we characterize several popular Bluetooth-to-serial modules used in skimmers for wireless data exfiltration. On the Bluetooth side, a Bluetooth-to-serial module provides a Serial Peripheral interface, which most operating systems recognize as a Bluetooth modem and instantiate a serial device for it. Operating systems will create a corresponding serial device, allowing user-space applications, namely a criminal’s card dumping application, to communicate with the module. On the hardware side, a Bluetooth-to-serial module provides a TTL-level receive and transmit pin, allowing it to interface to any micro-controller UART. The module this allows even the simplest micro-controller to communicate via Bluetooth with a host device. The 2.4GHz Bluetooth antenna is included on the module’s circuit board (exposed area to the left of the metal shield for the module shown in Figure 1), so the antenna is also hidden.

Bluetooth-to-serial modules generally require no configuration, however, most can be reconfigured using Hayes-style modem AT commands. In Section 4.2 we describe the configuration capabilities of popular modules. Notably, all of the Bluetooth-to-serial modules we found in skimmers support changing the device MAC address, Bluetooth device name, changing the pairing password, and the ability to become non-discoverable once paired.

2.2 Economics of Carding

Stealing and monetizing stolen credit and debit card data, called carding by its practitioners, is a well-studied form of financial fraud. Skimmers are just one of the ways of obtained card data, along with stealing credit card information from consumer devices or stealing payment information databases from merchants and payment processors. The skimmer installer’s revenue per skimmer, as well as consumer, merchant, and bank losses, depend directly on the expected value (revenue/loss) per card and the numbers of
For skimmer installers, there are two ways to cash out stolen credit card data: selling it on the black market or re-selling it. Reported cash-out values for credit cards fall in the $20–220 range, depending on whether the card is a debit or credit card, and whether it comes with a PIN (for debit) or billing ZIP code (for credit). Table 1 provides a summary of these prices with references. The second option for monetizing stolen credit card data is to cash it out yourself. Debit cards with a PIN are cashed out by withdrawing money from an ATM, while credit cards are cashed out by purchasing high-value merchandise (e.g. iPhones) and re-selling it. Reported cash-out values for credit cards fall in the $400–1,000 range, depending on credit limit associated with the card, while industry-reported losses per card are estimated at $650 for debit cards and $1,003 for credit cards (Table 1). In the U.S., consumer liability for fraud is limited to $50 for credit cards by statute. Debit card liability limits range from $50 when reported within two days, to no limit if reported after 60 days. Finally, in prosecuted cases of credit and debit card theft, the per-card loss is estimated at $500 in most cases, the minimum recommended by U.S. Sentencing Commission Guidelines.

Daily card volume. The number of cards a skimmer captures per day depends on the number of cards transactions per day. This value is difficult to determine as skimmers can remain undetected for several days. Unfortunately, there is little reliable data on this. From our own experience, we know that a skimmer can remain in the field for upwards of six months without detection (Section 3.1).

2.3 Skimmers Recovered in the Wild

To understand the prevalence of skimmers in the wild, we obtained data on recovered skimmers from three regions in the United States: San Diego and Imperial counties of California, with a combined population of 3.5 million inhabitants along the border of the United States and Mexico; the state of Arizona, with a population of 7 million inhabitants; and the state of Florida, with a population of 21 million inhabitants. Table 2 summarizes the statistics. We note that these numbers do not represent all recovered skimmers. Specifically: For San Diego and Imperial counties, our statistics represent the number of skimmers found by or reported to a U.S. federal law enforcement agency office responsible for those counties. For Arizona and Florida, our statistics represent skimmers found by or reported to the Arizona Department of Weights and Measures and the Florida Department of Agriculture and Consumer Services.

From the table it can be observed that the number of recovered skimmers has increased from 2016-2018 in both Florida and Arizona. The total number of skimmers recovered in 2018 across the three geographic regions is significant, as the total monetary impact from these skimmers alone would be 17.43 million USD per day. And yet as the skimmers per million people number shows, the possibility of an average consumer encountering a skimmer at a gas station is quite small.

### Table 1: Stolen credit and debit card valuation. All prices in U.S. dollars.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Value</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Black market price</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debit, no PIN</td>
<td>$20–30</td>
<td>[28, 40, 16, 37]</td>
</tr>
<tr>
<td>Debit with PIN</td>
<td>$110–220</td>
<td>[25, 40, 37]</td>
</tr>
<tr>
<td>Credit, no ZIP</td>
<td>$10–25</td>
<td>[28, 40, 16, 37]</td>
</tr>
<tr>
<td>Credit with ZIP</td>
<td>$25–60</td>
<td>[28, 40, 16, 37]</td>
</tr>
<tr>
<td><strong>Cash-out value</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit (standard)</td>
<td>$400–800</td>
<td>[15, 19, 31, 44]</td>
</tr>
<tr>
<td>Credit (premium)</td>
<td>$1,000</td>
<td>[19, 10, 29]</td>
</tr>
<tr>
<td><strong>Bank and merchant loss</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit</td>
<td>$1,003</td>
<td>[1]</td>
</tr>
<tr>
<td>Debit</td>
<td>$650</td>
<td>[9]</td>
</tr>
<tr>
<td><strong>Consumer liability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debit (&gt; 60 days)</td>
<td>unlimited</td>
<td>15 USC 1693g</td>
</tr>
<tr>
<td>Debit (&lt; 60 days)</td>
<td>max $500</td>
<td>15 USC 1693g</td>
</tr>
<tr>
<td>Debit (&lt; 2 days)</td>
<td>max $50</td>
<td>15 USC 1693g</td>
</tr>
<tr>
<td>Credit</td>
<td>max $50</td>
<td>15 USC 1643</td>
</tr>
<tr>
<td><strong>Prosecuted loss</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit or debit</td>
<td>$500</td>
<td>[7]</td>
</tr>
</tbody>
</table>

The number of cards a skimmer captures per day depends on the number of cards transactions per pump per day, which will vary by station. Rippleshot, a payment fraud prevention service, states, “a single compromised pump can capture data from roughly 30–100 cards per day” [6], which agrees with the estimate of 20–50 cards per day we received from U.S. law enforcement agents. Finally, in 10 skimmers recovered from the field, from which law enforcement agents believe data was collected daily, we found an average of 20 card tracks per skimmer, divided evenly between debit and credit cards.\(^4\)

**Skimmer lifetime.** Because internal fuel pump skimmers draw power from the PoS circuitry, they are not limited by battery life and can remain operational indefinitely. Skimmer lifetime, then, is limited only by how long they can remain undetected. Unfortunately, there is little reliable data on this. From our own experience, we know that a skimmer can remain in the field for upwards of six months without detection (Section 3.1).

**Total skimmer value.** At $500 per card and 30 cards per skimmer per day, the daily value of an operating skimmer is about $15,000 per day, or $450,000 per month. Even at the low end, $400 per card at 20 cards per day, a month of operation results in $240,000 per month.

\(^4\)These skimmers were provided to us because they were removed by the station owner, rather than law enforcement, making them unsuitable for use as evidence.
3 Data Collection

Driven by the observation that skimmers are rare—most gas pumps do not have skimmers installed in them—we created a tool to evaluate the effectiveness of passively detecting if a gas station has a skimmer by scanning for the Bluetooth modules on the skimmers. We begin by presenting an overview of the Bluetooth scanning tool. Then, we describe the importance of designing the tool to direct users to perform more data collection when suspicious devices were detected that may be skimmers. Next, we describe how we identify skimmers in the data collection.

3.1 Bluetana: Crowdsourcing Skimmer Scans

Our tool, called Bluetana, is an Android application that we provide to officials and volunteers to scan for skimmers at gas stations. Bluetana collects Bluetooth scans and geo-location data, and immediately uploads it to our secure database. Bluetana repeatedly scans for nearby Bluetooth (both Classic and Bluetooth Low Energy), devices every 5 seconds using Android’s Bluetooth API. It collects all of the Bluetooth scan data that Android makes available, including: Device name, MAC Address, Class of Device, and signal strength. This indiscriminate data collection proved to be valuable: we discovered that skimmers all have the same Class of Device: “Uncategorized” (Section 4.2). Class of Device information is not considered by any of the Bluetooth skimmer scanning applications we tested.

How we visited 800 gas stations. We outfitted 44 volunteers and fuel station inspectors in six U.S. states (CA, AZ, MD, NC, NV, IL) with low-end smartphones running Bluetana in kiosk mode (they could not close the application). We selected officials who frequent gas stations as part of their daily job duties, primarily, they were Weights and Measures officers.

Indicating suspicious devices to inspire data collection

The Bluetana display shows a list of Bluetooth devices detected in scans. When Bluetana detects a device that could be a skimmer, it indicates this to the user by highlighting a device in the list (Figure 3). If a device is highlighted in red, it indicates that it matches all of the properties of the recovered skimmers we observed (detailed in Section 4.2). If a device is highlighted in orange, it indicates that this device matches some of the properties of a skimmer, but that one of the properties indicates it may be a legitimate product using the same Bluetooth module as a skimmer. During the course of the study, we constantly refined our understanding of what skimmers looked like in Bluetooth scans. Therefore, we designed Bluetana we can remotely update it to indicate the latest profile of skimmers that we had developed.

This simple highlighting proved to be vital to our data collection. It inspired our users to collect more signal strength samples, and even perform inspections (if they had the authority).

For example, an Arizona Weights and Measures inspector was driving by a gas station with Bluetana running, when two red highlighted devices appeared. He made an unscheduled stop at the gas station, performed a skimmer inspection, and discovered two skimmers. Figure 4 shows a portion of the official Arizona inspection report documenting this inci-

---

5 Indeed, we observed many legitimate devices using the same Bluetooth modules as skimmers (Section 4.3)
Identifying skimmers after data collection

During the study, we manually examined every Classic Bluetooth device observed at a gas station visit in real time (as Bluetana users upload their scan data). At first, we relied primarily on the signal strength of the device to determine if it was a suspected skimmer. By the nature of being installed inside a gas pump, the Bluetooth signal of a skimmer is strongest in the pump area. Other devices that we suspected may be skimmers all had a low signal strength in the pump area, because aside from the cars parked at the pumps, the only places where a Bluetooth device would be located in the pump area would be inside the pump. Combining the signal strength with the geo-location from GPS, and satellite imagery of the gas station, we were able to easily detect when the signal was emanating from inside of a gas pump (example shown in Figure 5). While at a gas station, Bluetana users also noticed this by moving toward the pump area to see if the device’s signal strength increases.

If we saw any suspicious devices in the dataset, we alerted officials that they should inspect the pumps at the station in question. Initially, we did not know which of these devices were skimmers; many initial inspections we requested turned up empty handed. However, as the study progressed, and we improved our understanding of the properties of skimmers, having a database of all prior scans made it possible for us to look for skimmers that we may have missed in the past.

In particular, looking back in at the database lead to us to discover two skimmers that we missed. A retroactive analysis of two stations discovered skimmers that were still operating even though we first detected them six months earlier. This natural experiment is likely the first concrete data on how long skimmers can be installed without being found in a routine or complaint-induced pump inspection.

3.2 Why doesn’t Bluetana connect to devices?

We could collect more data about Bluetooth devices by trying to connect to them. This could be useful for conclusively detecting a skimmer, information about the type of Bluetooth device, and even sending it commands that skimmers are known to respond to, to see if it responds in the same way that known skimmers do. This is precisely what one of the current Bluetooth skimmer scanning applications on the play store does.

This practice may seem innocuous, but our discussions with law enforcement indicate that this could overwrite information critical to future investigations. The problem is, the firmware in many skimmer Bluetooth modules records the last-paired MAC address. This information can be used to link a suspect possessing a smartphone or laptop with their skimmers. The typical forensic evidence collection performed by law enforcement on skimmers includes collecting the last-paired MAC address [41].

3.3 How does Bluetana compare to other skimmer detection applications?

Bluetana is designed primarily to perform the large-scale measurement study presented in this work. It is not intended as a tool that consumers can use to detect skimmers. This is why it indiscriminately collects all the information possible from the Android API. In essence, Bluetana evaluates the heuristics used by other detection applications, such as only flagging devices that match a MAC Address prefix or device name of recovered skimmers.
4.1 Dataset Overview

In Table 3, we provide a summary the number of Classic Bluetooth devices that we observed in each state. We focus our study on Classic Bluetooth devices because those are the only modules known to be used in gas station skimmers at the time of the study. In Section 5.1, we describe how criminals shifting to using BLE devices may make it much more difficult to detect their presence with scans.

Over the course of the year-long study, Bluetana users visited 780 gas stations across four states. Although a total of 1,590 Bluetooth Classic devices were found in Bluetana scans, there were only an average of 2.05 Bluetooth Classic devices seen per station ($\sigma = 2.1$). Given that there are only a small number of Bluetooth devices seen per station, it may seem likely that these devices are likely to be skimmers. However, only a small fraction (4.25%) of these suspect devices matched the profile of skimmers. In fact, only 17 gas stations were found to have skimmers installed.

4.2 What Do Skimmers Look Like in Scans?

Next, we present the results of how skimmers appear in Bluetooth scans. Specifically, we describe the features of the 37 skimmers that we discovered during the course of this study.

**Bluetooth modules used in skimmers.** Skimmers typically use CSR (Qualcomm) chip-set-based Bluetooth modules. By default these devices to operate in discoverable mode, so they will appear on Bluetooth scans. Criminals can come up with creative strategies for temporarily disabling discoverable mode, but as we will discuss in Section 5.2 this makes it more difficult for the criminals to exfiltrate card numbers without evidence linking them to the crime. They also can change all of the properties that appear in scans with varying level of difficulty\(^7\), we observe that they change only the device name, the others are either set to default at manufacture.

The default properties of these modules are:

<table>
<thead>
<tr>
<th>Mod.</th>
<th>MAC Prefix</th>
<th>Dev. Name</th>
<th>Class of Dev.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RN</td>
<td>00:06:66</td>
<td>&quot;RN&quot;</td>
<td>Uncategorized</td>
</tr>
<tr>
<td>HC</td>
<td>(98:D3:31)</td>
<td>&quot;HC&quot;</td>
<td>Uncategorized</td>
</tr>
</tbody>
</table>

The Bluetooth characteristics of the skimmers that we saw in the wild are provided as an overview in Table 4. For this analysis, we added an additional 10 skimmers beyond the 37 that Bluetana that were provided to us directly by law enforcement investigators\(^6\).

Unfortunately, many of these apps attempt to pair with the device, which as was discussed earlier, is problematic for investigators\(^6\).

---

\(^6\)This is one of the reasons we did not include the Service Discovery Protocol in our fingerprinting.

\(^7\)Changing the module’s MAC address (bdaddr) requires a SPI wire connection to the device and a proprietary configuration application from CSR.
Table 4: Breakdown of characteristics seen in the skimmers recovered during our study. Bracketed names are abstractions on the names the devices actually had, for preservation of privacy.

<table>
<thead>
<tr>
<th>Bluetooth Scan Property</th>
<th># of skimmers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class of Device</strong></td>
<td></td>
</tr>
<tr>
<td>Uncategorized</td>
<td>47</td>
</tr>
<tr>
<td><strong>Device Manufacturer (IEEE OUI)</strong></td>
<td></td>
</tr>
<tr>
<td>Roving Networks</td>
<td>27</td>
</tr>
<tr>
<td>Shenzhen Bolutek</td>
<td>1</td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>20:13:01</td>
<td>1</td>
</tr>
<tr>
<td>20:17:11</td>
<td>1</td>
</tr>
<tr>
<td>20:18:01</td>
<td>2</td>
</tr>
<tr>
<td>20:18:08</td>
<td>13</td>
</tr>
<tr>
<td>20:18:09</td>
<td>1</td>
</tr>
<tr>
<td>98:03:35</td>
<td>1</td>
</tr>
<tr>
<td><strong>Advertised Name</strong></td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>31</td>
</tr>
<tr>
<td>[Law enforcement]</td>
<td>2</td>
</tr>
<tr>
<td>[Mobile phone]</td>
<td>2</td>
</tr>
<tr>
<td>[Indescribable object]</td>
<td>1</td>
</tr>
<tr>
<td>[Numerical]</td>
<td>2</td>
</tr>
<tr>
<td>Unnamed</td>
<td>9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>47</td>
</tr>
</tbody>
</table>

All of the skimmers have an “Uncategorized” device class

Class of Device is an often overlooked field in a Bluetooth scan, because it only is used by Bluetooth devices to add icons to the scan list to show the type of device (e.g., Headphones). Criminals do not appear to be modifying the Class of Device: all 47 skimmers we scanned used the default “Uncategorized” device class. Changing device class is easy: the Bluetooth modules have a simple serial command to change it. None of the Bluetooth scanning tools that we are aware of record Class of Device. Nor do the applications that claim to be developed specifically for scanning for Bluetooth skimmers (e.g., SkimPlus [38]).

MAC prefixes are often defaults

The MAC address is burned into the ROM of the Bluetooth device when it is manufactured. Although it is possible to change the MAC with a fairly complicated SPI-based reprogramming of the CSR chip’s EEPROM, however, we have seen no skimmers where this was done.

The first three bytes (prefix) of the MAC address prefix reveal the manufacturer of the device, several skimmer detecting applications use this as the primary way of detecting skimmers. In its proper use, MAC address prefixes are assigned by IEEE. All of the RN Bluetooth modules have the same manufacturer MAC prefix that is assigned by the IEEE to “Roving Networks”, the HC modules have a wide variety of MAC prefixes: all but one are not known to the IEEE.

This could make it significantly more difficult to detect an HC-equipped skimmer. However looking at all of the prefixes that are Unknown, a clear pattern emerges. The manufacturers appear to be burning the date of manufacture into the first four bytes of the MAC address in the following format: YY:YY:MM:DD. In Section 6.2 we show that we can use manufacturer MAC assignment patterns like these to determine if several Bluetooth modules with similar MAC address may be from the same crew.

Device names are often default, occasionally customized

Bluetooth device names are a way for users and manufacturers a friendly name for users to easily select their device in Bluetooth scans. Criminals often do not change the default name that module manufacturers program at the factory. This could make the devices look innocuous, particularly because these modules are often set with default names in legitimate products. Some criminals do change the device name in what appears to be an attempt at making the skimmer look innocuous: we observed a wide variety of names from number sequences, to making the skimmers look they were run by law enforcement. These actually have the opposite effect of what the criminals intended: they make easier to detect as skimmers, because is uncommon to see a Bluetooth module with a customized name.

For several skimmers, we did not observe a device name. This is likely because the name packets may not be retrieved properly due to poor signal conditions when the device was observed. The name requires sustained signal quality because it is exchanged at a later stage in the Bluetooth scanning process (as a response to the remote name request packet), and it requires two packet exchanges.

Most skimmers are detected within one minute of arriving at a gas station

Being installed in the metal enclosure of gas pumps limits the Bluetooth range of skimmers, and Bluetooth scans can take up to 20 seconds to complete. Therefore, one may expect that receiving the first Bluetooth scan respond from a skimmer may not occur until the Blueta device has moved very close to the pump with the skimmer. To evaluate this, we observed the first point when the officials driving within 150 feet of gas station first detected the skimmers that were there. 80% of the skimmers were detected within one minute of arriving at a gas station, with a median of 12 seconds. Compared to the average of 30 minutes that inspectors take
to check if there are skimmers in all of the pumps gas station, this is a 99% decrease in search time, allowing inspectors to passively check gas stations for skimmers as they do other activities at the station (e.g., inspecting the pricing at the convenience store).

### 4.3 Are skimmers hidden in scans?

Finally, we present the results of our large-scale study of how easily skimmers can be detected in Bluetooth scans. By scanning for Bluetooth devices while visiting 780 gas stations across five states, we have captured a large sample of what the Bluetooth environment looks like near a typical gas station. In this study, we compare the properties that the 37 skimmers we detected have in Bluetooth scans, with the other 1,590 devices Bluetana observed at the gas stations.

The primary result of this study is that skimmers are not well hidden today: even though many skimmers use the default configuration of their Bluetooth modules. We conclude that by combining multiple characteristics: MAC prefix, Class of Device, and device name, there are only a small number of devices that could be confused with skimmers. Also, criminals appear to be making it easier to detect their skimmers when they creatively modify their skimmer’s device name.

On the other hand, this study also reveals that there are ways that criminals could hide themselves better in Bluetooth scans. For example, they could change the Class of Device and hide as a more popular device such as a smartphone to make it much more difficult to detect.

**Skimmers are uncategorized, but so are many other devices**

The only Bluetooth property that is common among all skimmers we observed, is that they have an “Uncategorized” Class of Device. Yet, in Figure 7, we see that, surprisingly, Uncategorized devices are commonly seen at gas stations: they are 20.8% of the total number of devices seen across all gas stations. By filtering to include only the devices which are Uncategorised, we reduce the number of stations with suspect devices to only 218 (from 780).

**Legitimate devices use the same modules as skimmers**

Within Uncategorised devices, we next look at the MAC prefix to see if the manufacturers of Bluetooth modules used in skimmers are common. This is an important observation, particularly because many skimmer detection applications only indicate the presence of a skimmer by matching the prefix of the MAC address. Of the devices that had the same MAC prefix as skimmers we observed, only 98 devices matched these MAC prefixes (out of 353 Uncategorised devices). This reduces the number of stations where there could be skimmers to 81 out of 780.

Figure 8 shows that more than half (20) of the Roving Networks devices seen at gas stations were skimmers. We grouped all devices with rare MAC prefixes into a single group, MAC prefixes with less than five devices, one of the skimmers fell into that category. There were also many devices with MAC prefixes unknown to the IEEE, many of which were not skimmers.

---

*Source: discussions with inspectors*
Default and custom names are mostly skimmers

After filtering devices by OUI and device class, we are left with 98 devices, 27 of which are skimmers\(^\text{10}\). The last field we study is the Bluetooth device name (Figure 9). The criminal’s practice of leaving the name as default appears to make the skimmers much easier to detect, as few legitimate products that use these Bluetooth modules use the module’s default name. Surprisingly, only four skimmers disguised themselves as other products or custom nondescript (or even descript) names, and the product-named skimmers are well hidden, but the custom names are not. Many devices (and skimmers) did not have a name in the Bluetana data, this is why we fall back to signal strength localization techniques when looking for skimmers.

5 Counter Measures and Responses

The current work is a single snapshot in an evolving landscape of attacks on payment systems. While Bluetana has proven effective at finding Bluetooth skimmers, it by no means represents the last move in the cat-and-mouse game. In the remainder of this section, we discuss what the next few steps in this arms race might look like. That is, given that inspectors and volunteers are using Bluetana, what is the skimmer installers’ next move, it’s cost, and what our response might be.

5.1 Switching to Bluetooth Low Energy

We have observed that by switching to BLE, criminals have many more places to hide. Figure 10 shows the cumulative distribution of the number of BLE and BC devices we saw at each fuel station. Under the filtering of Section 4, over 5,000 unique BLE devices were seen, making the ratio of Classic to BLE approximately 1:3.

Cost to attacker. There is almost no cost to criminals in switching their Bluetooth modules to BLE. In fact, newer EMV skimmers discovered in other countries are BLE enabled [24]. However, none of our contacts in law enforcement have encountered BLE-based gas station skimmers. It is possible that there is simply no incentive to switch: the same reason criminals have not yet adapted to masking their Bluetooth device class.

Response. BLE devices may be harder to differentiate due to the higher number of devices at each gas station and a lack of distinguishing features. 86.6% of BLE devices we saw had an uncategorized device class. With more sophisticated filtering techniques, it may still be possible to isolate BLE skimmers within. One possibility is automated RSSI

\(^{10}\)We do not include 10 of our skimmers in this analysis because they were detected on the second visit to a gas station.
5.2 Non-Discoverable Skimmers

The most natural way to evade discovery via Bluetooth would be to put the module in non-discoverable mode. When a Bluetooth device is non-discoverable, it does not respond to normal discovery enquiries. Instead, it only responds to paging packets addressed to its MAC address.

**Cost to attacker.** Non-discoverability would make exfiltration more difficult for criminals. One possibility is creating a pre-paired data collection device. However, we have been informed by law enforcement that the individual who installs the skimmer is often independent from the individual responsible for data recovery (called a “mule”). The criminal would not be able to send a mule to recover card data without first delivering them the device. Alternately the criminal could record the MAC address of the skimmer Bluetooth module. This would require careful bookkeeping and the use of tools that support the creation of a non-discoverable connection.

**Response.** It is still possible to discover a non-discoverable device. For a small set of target address ranges, e.g., \( \text{00:06:66} \) used by Roving Networks modules, we believe it would be practical to attempt to guess all 16.8 million possible addresses. Prior work has shown that it is possible to discover any non-discoverable device via brute force in 18.64 hours; knowledge of OUI would ideally allow us to halve this [14]. Unfortunately, this would require specialized hardware, rather than an inexpensive Android phone.

5.3 Impersonating Common Benign Devices

Another natural response to Bluetana would be to change the MAC address and name of the device to that of a common benign device, such as a mobile phone or a Bluetooth-enabled car entertainment system. This would make the skimmer appear innocuous to Bluetana.

**Cost to attacker.** Reprogramming the MAC address on the CSR-based Bluetooth modules, which include the Roving Networks and HC-05 and HC-06 modules, cannot be done using the AT commands used to change device name and pairing. Instead, the skimmer installer would need to reflash the CSR firmware using a special programming cable. While, in principle, not difficult, it would require an additional degree of sophistication than programming a simple micro-controller development board. The skimmer installer could also change the device name but not the MAC address, say, to one of the known benign devices using the same module, something that us possible to do by issuing AT commands from the micro-controller to the module. While this would confuse Bluetana, it also runs the risk of confusing the skimmer installer by making many benign devices appear to be a skimmer.

**Response.** Because Bluetana collects all Bluetooth data, we can identify skimmers retroactively when we learn of a new MAC address and name used by known skimmers. Thus, if attacks switch to impersonating benign devices, we can update the Bluetana hit list and white list to identify those devices as suspicious. This would result in additional inspections, but would still provide significant gain over the state of the art.

5.4 Using Non-Bluetooth Communications

During discussions with law enforcement agencies tasked with identifying skimmers, we were told about skimmers that use GSM modems or WiFi as an alternative to Bluetooth. In the case of WiFi, we believe that the Bluetana methodology will still be effective. GSM poses a more serious challenge for detection.

**Cost to attacker.** While using GSM would avoid detection using Bluetana, it creates an additional trail of evidence linking the perpetrator to the skimmer. Law enforcement officers could obtain information about the SMS recipient through subpoenas, so receiving the SMS messages on another phone on a US carrier, for example, would be easy to trace. The perpetrator would need to use an SMS service that would not expose his/her identity.

**Response.** In addition to legal tools available to law enforcement to trace SMS messages, a GSM modem could be detected using a software-defined radio, including a low-cost ($10) RTL-SDR dongle.
5.5 Attacker Bottlenecks

The attacker (skimmer installer) has several practical ways to evade detection using Bluetana. Each of these, however, has an additional cost to the attacker in terms of effort, risk exposure, or expertise. We do not yet have a strong understanding to which of these costs attackers are most sensitive. Indeed, the very low price of stolen credit card numbers, compared to their potential cash out value (Table 1) suggests that the bottleneck in the carding value chain is not getting card information but cashing out cards. Thus, while Bluetana may raise the cost for attackers, we do not believe that it will raise it so much as to make fuel dispenser skimming unprofitable.

6 Operational Lessons Learned

While performing the Bluetana study, we learned several lessons about the operational use of Bluetooth scanning for skimmer detection. In this section, we provide an overview of two most important lessons we learned.

6.1 Bluetooth helps during inspections

Criminals hide skimmers in the crevices of gas pumps to avoid detection during inspections. We witnessed several instances where inexperienced investigators were unable to locate the skimmers and therefore they ended the inspection. Once, investigators started an inspection because Bluetana flagged four devices near a gas station. After a careful inspection, they were not able to locate the skimmers. They reported this to law enforcement, and we double checked the data, and it appeared that there were in fact skimmers at the station. Then, law enforcement officials who have experience in skimmer recovery arrived, and after performing a second thorough inspection of the station, they discovered the four skimmers. The evidence provided by Bluetana forced them to continue the inspection, instead of abandoning it and leaving the devices in the field.

Figure 11 demonstrates an instance of how the signal strength measurements helped inspectors determine which pump had a skimmer. When the gas pump’s metal door was opened, the signal strength increased significantly, prompting inspectors to look for the skimmer in that pump.

<table>
<thead>
<tr>
<th>Group</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of skimmers</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Seen across stations</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Min. distance in MAC address</td>
<td>17</td>
<td>166</td>
<td>9</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Min. distance between closest MACs (miles)</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>448</td>
</tr>
</tbody>
</table>

Table 5: Geographically separated skimmers often had close MAC addresses.

6.2 MAC address patterns reveal the source

Network equipment vendors (e.g., Bluetooth module manufacturers) allocate MAC address to their products sequentially off of the assembly line [27]. Therefore two devices having very close MAC addresses, mean they are very likely part of the same batch of devices sold. This information can be used to associate skimmer Bluetooth modules to the same builder or crew.

By grouping the skimmers recovered using Bluetana up to the last byte of their MAC address, we see six different groups of MAC addresses which are shown in Table 5. Groups 1 and 2 were found at the same gas station, which is expected as criminals often install multiple skimmers. Groups 3–5 were seen across 2 different stations separated by over 16 miles in the same county. Criminals are known to plant skimmers across multiple stations in the city/county, and these patterns are revealed in the MAC address data. Group 6 was the most interesting: the closest MAC addresses were in different cities separated by 448 miles. This may seem surprising, but often skimmer crews migrate from city to city installing skimmers to avoid detection.

7 Related Work

External Skimmer Detection. SkimReaper, a foolproof mechanism for the detection of magnetic read head based external skimmers is effective in detection [39]. This mechanism works by exploiting the physical property of magnetic stripe readers, which require the magnetic stripe to come in physical contact with the read head. Skim Reaper is therefore able to figure out if an extra read occurred (which means an external skimmer is attached). The PCI Security Standards Council have also released guidelines for the prevention of external skimming [13].

Our work complements these existing systems. Many external skimmers are Bluetooth enabled to allow for discrete data retrieval [33]. Additionally, no current system allows for the accurate detection and analysis of internal skimmers.
Bluetana demonstrates the ability of Bluetooth to provide an alternative to the manual inspection of the pumps.

**Bluetooth.** Our work is a novel application of the Bluetooth protocol; it relies on prior work done in the realm of localization and discovery.

Signal strength-based localization is well studied. Prior work on Bluetooth position using Android smartphones has shown that RSSI retrieved during an inquiry scan may be used to accurately estimate the positions of devices [26, 45]. We use the techniques pioneered in this work to localize and determine whether a skimmer is inside of a gas pump.

In addition, we rely on results established by prior research on device discovery and optimal scan time. Studies of discovery time in moving vehicles and static observers have demonstrated that device discovery times are often far shorter than the approximately recommended by the Bluetooth standard. [30, 36, 18] This related work has allowed us to reduce the amount of time that we spend scanning while remaining confident in our ability to discover potential skimmer devices.

**Inventory Attacks.** The unwanted discovery of the existence of a device is referred to as an inventory attack [46]. Prior work on fingerprinting and discovery attacks has focused on the realms of RFID, web browsing, and Bluetooth Low-Energy [42, 43, 17]. In this research, we invert the traditional inventory attack to violate the privacy of adversarial Bluetooth devices and protect the privacy of consumers.

8 Conclusion

This paper presented Bluetana, a empirical measurement study of Bluetooth’s ability to detect internal card skimmers. Bluetooth makes it possible to quickly and accurately detect skimmers within gas dispensers. Our evaluation has shown that Bluetooth is a promising method of skimmer detection, capable of detecting 37 skimmers for a daily monetary impact of $555,000 in a study of 780 stations.

The problem of skimming will only grow in coming years. Push-back from banks and card issuers has led to wide scale adoption of EMV in traditional POS systems. However, gas stations have not adapted. We randomly sampled 0.5% of all gas stations in the US and classified pump payment technology. Google Street View images of the dispensers revealed that as of the current date only 13.8% of gas stations have retrofitted EMV readers and only 1.6% have installed EMV based dispensers.

References


