Skimming: Attacking Your Financial Security

S. Shaw

Comp 116: Computer Security

13 December 2019

Abstract

Digital currency has a substantial presence in today's economy, especially with the growing number of electronic transactions consumers make to purchase products and services from online sellers. These electronic transactions present many security challenges for businesses and financial institutions. Namely, it is harder than ever for businesses to validate a consumer's identity and determine whether a payment is legitimate. Banks experience even greater challenges because consumers depend on them to safeguard their money from fraudulent actors. Banks and credit card companies implement a number of hardware security measures (e.g., card chips, ATM tech.) to detect and prevent illegitimate access to funds. First, this paper investigates how these security features have evolved to prevent attacks, and the techniques attackers use to exploit security weaknesses. Then, it makes recommendations about how to defend against such attacks and how technology can be improved to protect consumers.

1 Introduction

Currency has moved into the digital realm – generally, for the better. Digital currency has enabled e-commerce to expand to a trillion dollar industry over the course of a few decades. Today's consumers have unprecedented access to a global economy; this access has undoubtedly enabled businesses to grow and technologies to develop rapidly. Although digital currency disburdens the consumer and business during a transaction, the ability to "carry" large sums of money, via remote access, presents significant security risk. It's now harder than ever for businesses and financial institutions to validate a consumer's identity; these vulnerabilities have opened the doors for new types of identity theft and fraud.

To protect clients, banks continually develop more advanced security features. Without a client's trust, a bank cannot do business. Modern hardware security measures (e.g., card chips, ATM tech.) help detect and prevent illegitimate access to funds – but they aren't infallible. Card skimming involves an perpetrator using a device – called a skimmer – to harvest details from a credit or debit card [12]. With these details, criminals can potentially create cloned cards – illegitimate cards using a legitimate user's stolen information – or gain access to funds via other means.

2 To the Community

For better or worse, the world revolves around money – for living essentials, opportunities, etc. With technologically-advanced, computerized banking, the risks are higher than ever; the added complexity of this technology introduces new potential exploits. Nevertheless, almost everyone relies on this technology to safeguard their livelihood. It's essential to keep our money well-protected, and, to do that, one must be educated on the latest security measures and flaws. Every time a consumer makes a transaction, private information is transmitted – communicated in one way or another – giving perpetrators an opportunity "listen in". More specifically, in order to understand how criminals can extract information from unsuspecting victims, it's important to understand how user information is stored on cards and how it is transmitted during a transaction. By understanding how criminals can skim your information, you are in a better position to protect it.

3 Credit and Debit Cards

Although we have increasing financial control (e.g., bank apps) via our mobile devices, physical cards are still used as a quick way to authorize transactions. Card technology has become increasingly more advanced with time to provide additional security, but threats remain.

3.1 Magnetic Stripe

Early credit cards stored information necessary to conduct an electronic transaction on a magnetic stripe: cardholder name, card number, card expiry date, etc. [13]. This technology was introduced in 1970 by IBM; the year before, IBM engineer Forrest Parry worked on combining a magnetic stripe with a standard-issue identity card for the CIA [7]. Although the technology has become widespread due to its low cost, this decades-old magnetic strip (or "magstripe") technology presents security risks.

Accessing information on magnetic stripe cards and creating cloned cards is trivial. MagSpoof is a modern magstripe card spoofing technology; it produces an electromagnetic field that emulates the magnetic signature of a card as it's swiped through a terminal [6]. This implementation enables Magspoof to wirelessly imitate cards (i.e., the device will cause a terminal to detect a card swipe if the device is placed in close proximity – no swipe required) even if the card reader is "swipe only". Additonally, MagSpoof can disable chip and PIN protection. The simple schematic to build a MagSpoof device, which can be about the size of a quarter (shown in Fig. 1), is available publicly online – as is the firmware.

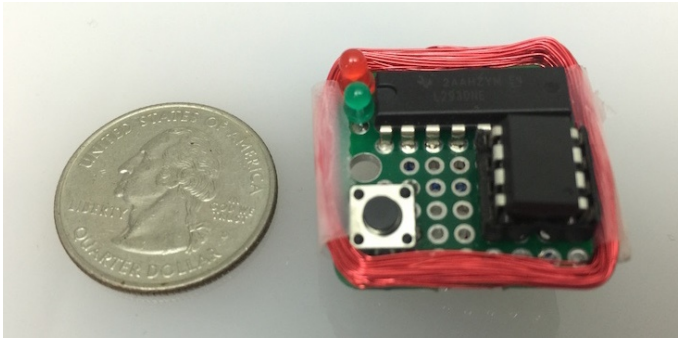

Figure 1: Hardware implementation of a MagSpoof device [6].

3.2 EMV – Chip and PIN

EMV is a standard originally designed by Europay, Mastercard, and Visa that governs cards with integrated circuits used for authorization [8]. EMVCo is an "international standards body that manages EMV technology standard for global interoperability of chip payment cards and acceptance devices." "Chip and PIN" cards are one type of transaction technology that meets EMV standards [3].

Although EMV cards provide more security than magstripe, skimming data from EMV card chips is still possible. When an EMV chip card is inserted into a terminal, the terminal makes physical contact with the chip and provides power to an integrated circuit which holds important user information. Instead of detecting a magnetic signature, terminals can send commands to the chip to access data. One available command is to verify the PIN associated with the card. However, to unlock the card, it is not necessary to verify the PIN; other commands can be run to read the data (pretty much all the data you would need to clone the card) without ever verifying the PIN [16]. Then, in some cases it is possible to create a magstripe card with the data harvested from the EMV chip card. As is well known, magstripe is still widely accepted.

However, cloning chip cards has become increasingly challenging. There are two classes of EMV chip cards. Older EMV cards are hardware-limited and use static data authentication (SDA). The communication between SDA cards and a terminal is cleartext, which leaves room for attackers to conduct a man-in-the-middle attack. Differently, newer cards use dynamic data authentication (DDA); these cards feature an encryption co-processor which allows encrypted communication [16].

EMV-compliant technology offers significantly greater security for transactions where the physical card is dipped into a reader. However, this technology's security benefits do not apply for card-not-present transactions (e.g., online transactions) where the chip is not used; all the information needed to complete the transaction can be read off the card with the naked eye.

3.3 Biometrics – On-card Fingerprint Authentication

The future of card security technology could lie in biometrics. Recently, Visa and Mastercard have both announced biometric cards with embedded fingerprint sensors [9, 15] as shown in Fig. 2. Beyond the obvious benefit

that card-embedded fingerprint scanning presents, the transition to this new authentication method would be simpler than the transition from magstrip to chip-embedded cards. Unlike the prior transition, which required new payment terminals to interface with the cards, biometric analysis could be incorporated on the existing format of chip-enabled cards. Furthermore, this additional sensing is powered via the terminal – just as the card chip is; as Visa puts it: no charging required.

Figure 2: Payment with an EMV Biometric Card from Mastercard [9]. A user provides a fingerprint while the card chip is inserted into the terminal to authorize the transaction.

4 Automated Teller Machines

Although card technology has become better with time, modern cards still feature magnetic stripes for backwards compatibility; it has taken a long time for vendors to upgrade to EMV chip technology. As long as the magnetic stripe remains on cards, they are at risk of being skimmed [10]. Automated teller machines (ATMs) are often prime targets for planting skimmers and other information stealing devices. ATMs are often unattended and may have limited auxiliary security (e.g., cameras, being located behind a secured door, etc.). In order to be effective, thieves must steal both the information on the card and the associated PIN.

4.1 Hidden Skimmers: Extracting Data from Cards

As mentioned before, even modern cards with EMV chips steal bear the magnetic stripe, which can be trivially skimmed (note that skimming devices can also be used for SDA EMV chip cards) [16]. Often times, thieves use magnetic stripe skimming devices that fit over top of the official terminal casing, called overlay skimmers; these false fronts appear to be part of the terminal [1, 14]. An example of such a device is shown in Fig. 3.

Figure 3: An example of an overlay skimmer for an ATM [14]. This device fits over the card receptacle. Notice its similar shape and color, which helps avoid visual detection.

When an unsuspecting victim inserts a card, the card details read by the malicious skimmer before they are read by the terminal. These types of devices can be installed very rapidly – in just a few seconds; strong double-sided tape can securely hold an overlay skimmer to a terminal (which can also prevent it from being detected) [11, 14]. This allows them to be installed in plain sight (e.g., a gas station convenience store) [10]. Although overlay skimmers are commonly employed, there are other types of skimmers too.

Another type of skimmer is known as a "deep-insert skimmer." A deep-insert skimmer is a specialized unit that is engineered to fit inside a target payment terminal card slot [14]. These devices are hard to identify visually, and must be inserted and removed with a specialized tool. Such devices can either feature magstripe readers or EMV shimmers to conduct a man-in-the-middle attack on EMV chip cards [14, 16].

4.2 Hidden Skimmers: Extracting the PIN

Similar techniques can be used for stealing PIN information. False keypads can be engineered to fit cleanly over the real terminal keypad as shown in Fig. 4 [1, 14]. When a user enters their pin on the keypad, the device logs the key presses.

Figure 4: Examples of false keypads at ATMS, used to collect user PIN information [1, 14].

Another approach is to hide a camera on or around the ATM as shown in Fig. 5; if the user is not careful to cover their PIN as they enter it, a criminal will be able to extract the sequence of digits by reviewing the video [10, 14].

Figure 5: Examples of hidden camera video feed used to record the sequence of key presses for a user's PIN [2].

Later, the data from a keypad or camera video feed can be coupled with card data from a skimming device to have enough information to conduct a fraudulent transaction.

4.3 Card Stealing

Alternatively, thieves can plant faulty, malicious ATM machines that are aimed at stealing cards and PIN numbers. An unsuspecting victim may insert a card and enter its PIN, not knowing that the planted machine will not release the card; it will be collected by the thieves later.

5 Defenses

There are a number of defenses that a consumer can employ to keep personal details safe. The most straightforward rule is simple: when in doubt, avoid using a card. When paying, use cash, and instead of using an ATM, visit a bank location and see a teller. The beauty of paying with cash a consumer sees the money visually and knows exactly how much is changing hands. Furthermore, no identifying information is transmitted as part of the transaction, meaning that there is no opportunity for information to be compromised.

However, sometimes paying with cash isn't an option. Fortunately, paying with cash isn't the only way to avoid presenting a card, potentially revealing sensitive information to attackers. Major technology players, such as Apple and Google, have introduced cashless payment methods of their own in the form of phone apps [4, 5]. These apps work by storing a user's card details in a virtual wallet, and allow the user to pay without the physical card present; this gives no opportunity for card details to be collected by a planted skimming device. At the time of purchase, Google Pay transmits an encrypted card number rather than an actual card number, and Apple Pay uses a device-specific number and transaction code in place of a real card number. This type of implementation keeps personal details safe.

Nevertheless, sometimes its necessary to use a card. In these scenarios, it is important to carefully examine the card terminal. As discussed, skimming devices often cover the real casing of a device; feel the device to see if components are loose, and be weary if they are. Then, when entering the card's PIN to complete the transaction, cover the keypad with your hand to obscure the sequence of key presses from hidden cameras or onlookers; don't rely on existing shielding (e.g., plastic shields), since attackers can hide small cameras within these [14]. Similarly, guard your card number and security code too, since these are details an attacker needs to complete a card-not-

present transaction (e.g., online, phone, etc.). Finally, as a reactive measure, review card statements regularly to spot irregularities.

6 Conclusion

Although card security technology has improved dramatically in the recent years, there are still security threats. Thieves have become increasingly adept at designing skimming devices that when fixed to a terminal seamlessly blend in. This provides significant opportunity to obtain a large volume of card details, given the increasing number of digital transactions. But, as computational power grows (and becomes cheaper), card providers can develop even more secure on-card chip technologies. Additionally, with an unprecedented number of transactions made online rather than in stores, there is less opportunity for thieves to steal card details.

References

[1] All about skimmers. https://krebsonsecurity.com/all-about-skimmers/, 2019. Accessed on 2019-02-12.

[2] ABC10. Skimmers allegedly installing cameras, skimmer on atm. https://www.youtube.com/watch?v=mztUTCANJJ0, Mar 2019. Accessed on 2019-13-12.

[3] Smart Card Alliance. Emv 101: Fundamentals of emv chip payment. https://www.youtube.com/watch?v=Zv1DjtBwADg, May 2014. Accessed on 2019-02-12.

[4] Apple. Apple pay: Cashless made effortless. https://www.apple.com/apple-pay/, 2019. Accessed on 2019-13-12.

[5] Google. Google pay. https://pay.google.com/about/, 2019. Accessed on 2019-13-12.

[6] Faisal Hussain. Magspoof digitally clones the magnetic stripe of any credit card. https://null-byte.wonderhowto.com/how-to/magspoof-digitally-clones-magnetic-stripe-any-credit-card-0166495/, Nov 2015. Accessed on 2019-02-12.

[7] IBM. Magnetic stripe technology. https://www.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/, Dec 2010. Accessed on 2019-02-12.

[8] Julia Kagan. Emv. https://www.investopedia.com/terms/e/emv.asp, Jun 2018. Accessed on 2019-02-12.

[9] Mastercard. Mastercard biometric card. https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html, 2018. Accessed on 2019-02-12.

[10] ABC News. Why chip credit cards are still not safe from fraud. https://www.youtube.com/watch?v=gJo9PfsplsY, Apr 2016. Accessed on 2019-02-12.

[11] Nolen Scaife. IEEE Symposium on Security and Privacy. Kiss from a rogue: Evaluating detectability of pay-at-the-pump card skimmers.

https://www.youtube.com/watch?v=__HLouiAbCk, Jun 2019. Accessed on 2019-13-12.

[12] Kim Porter. How credit card skimming works - and how to avoid it. https://www.lifelock.com/learn-fraud-how-to-avoid-credit-card-skimming.html, 2019. Accessed on 2019-02-12.

[13] Emily Sorensen. The historical roots of electronic card machines. https://www.mobiletransaction.org/history-of-credit-card-machines/, July 2019. Accessed on 2019-02-12.

[14] Nolen Scaife. USENIX. Usenix security '18 - fear the reaper: Characterization and fast detection of card skimmers. https://www.youtube.com/watch?v=OXTX0faic_I, Sep 2018. Accessed on 2019-13-12.

[15] Visa. Fingerprint authentication moves from phones to payment cards. https://usa.visa.com/visa-everywhere/security/biometric-payment-card.html, 2018. Accessed on 2019-02-12.

[16] Ada Wise. Blackhat 2011, chip pin is definitely broken: Credit card skimming and pin harvesting in an amv. https://www.youtube.com/watch?v=JXHVhvR4G44, Feb 2015. Accessed on 2019-02-12.