*How EMV Chip Cards Have Improved Electronic Payment Security*

Reagan Leonard  
*Senior, Class of 2020*  
*Computer Science Major*Spartanburg, SC  
rpl@g.clemson.edu  
  
William Shope  
*Senior, Class of 2020*  
*Computer Science Major*North Charleston, SC  
wshope@g.clemson.edu   
  
Benjamin Joye  
*Senior, Class of 2020*  
*Computer Science Major*Charleston, SC  
bjoye@g.clemson.edu

# Introduction

This template, From the inception of credit cards, security and fraud have always been a major issue. Since October 2015 in the United States, EMV chips have been required to be accepted by businesses or else they would be held liable if any fraudulent activity occurred [3]. This is because EMV chips in cards provide significantly more security than their chipless counterparts. Without a chip, thieves are able to steal card information very easily. Magstripe cards hold their data statically, and anyone with a magstripe reader is able to store that data and write it onto a blank card, creating an exact copy. Chips, however, uniquely encrypt the information on every transaction, which makes it much harder to intercept the data [4].

There are two main reasons why EMV cards are superior in terms of security to the classic magnetic-stripe cards that have been around since the 1960s: 1) fraudulent cards with EMV chips are much more difficult to make than fraudulent cards with magnetic stripes and, 2) “the data on chip cards is constantly changing making it extremely hard to isolate and extract” [1]. For obvious reasons, it is much more difficult for a thief to manufacture a fake chip card than one with a magnetic stripe, simply because of the hardware involved; they would need to manufacture the chips. Magnetic stripes, meanwhile, are simply what they sound like: a magnetized section of the card that essentially holds the card’s ID number. This can be recreated much more easily than a chip because of the hardware involved in a chip. Furthermore, the software that a chip brings to the table—the sophisticated encryption that occurs on each and every transaction—provides another added level of protection to the cardholder that has made the EMV chip the obvious world leader in card payment technology [2]. This has inspired the electronic payment world to take a deeper look into how we can make e-payment even more secure through further innovations in card technology, NFC payment, and online payment via private applications.

Overall, this project will address the differences between the EMV chip card and a credit card with a magnetic strip and then transition to the remaining security vulnerabilities as well as potential solutions to those vulnerabilities. This will be done by conducting a thorough literature review from which these security vulnerabilities will be identified. One of these solutions that we devise will be extensively reviewed and form the main basis of the following scientific paper.

## General Information on Topic

The origins of what has come to be known as the modern-day credit card began in 1946. A banker named John Biggins created the “Charg-It” card in Brooklyn, NY [5]. Any purchases made with a Charg-It card were forwarded to the bank Biggins owned. The bank then reimbursed the merchant and obtained payment from the customer. This model of triangular transactions was subsequently known as the “closed-loop” system. In the beginning phases of these types of cards, purchases could only be made locally and only bank customers could obtain a Charg-It card. Then, in 1951, Franklin National Bank, also out of New York, issued its first charge card to its loan customers [5].

Several years later, in 1958, American Express, which is now one of the largest and most successful credit card companies in the world, launched its first credit card. In the years that followed, American Express would prove itself as one of the global competitors in this newly discovered credit card market. In 1959, they introduced the world’s first plastic credit card, which quickly made the existing cardboard and celluloid cards obsolete. Five years later, there were over 1 million American Express cards in circulation and they were accepted at over 85,000 merchants, both in the U.S. and abroad [5].

Back when using credit cards was still a very manual ordeal, the process of paying for something with a card was much more intricate than it is nowadays. In order for a transaction to be completed, the merchant would call the cardholder’s bank, then the bank would call the credit card company. Then the credit card company would have to have an employee manually look up the customer by name in order to check their available credit balance. This system was obviously very clunky and cumbersome for every party involved and was bound to be replaced by something more technologically advanced in the future. Of course, it was made obsolete by a computerized version of this process in 1973 which was designed and implemented by the first CEO of Visa, Dee Hock. Once this process was handled by computers, the transaction time went from an arduous several minutes to being able to be completed in under a minute.

## Relevance of Topic in Modern America

As you can see from the description of the rise of the modern credit card, we have certainly come a long way in the innovation of credit card usage. We have also come a long way in the security of electronic payment. However, this does not mean that we do not still have a long way to go in improving the security of credit card payments. While most new credit cards issued nowadays are EMV chip cards, there are still many Magstripe cards in use around the globe. Obviously, these cards are highly susceptible to the sorts of attacks that we will perform in our demonstration. But just like with everything online that is supposedly “secure”, attackers are always evolving with security technology and they are constantly coming up with new ways to break through security measures. This means that every card or online transaction will always be at some degree of risk to attackers. The best we can do is to try and stay one step ahead of them, and having an EMV chip card in the modern era is one way to do so. Therefore, our topic is one of extreme relevance in modern-day America, and elsewhere for that matter!

## Outline of our Demonstration

For our demonstration, we have purchased a cheap Magstripe card reader that connects to a computer via USB. Using this, we will be able to write a Linux script to take in the data from the card and separate that data into its respective fields based on the Magstripe card data architecture. With this, we would be able to create a counterfeit card with that same data, and then explain how this would be avoided if the transaction had been done with an EMV chip card instead.

# Background of magstripe cards

At the time of their creation, magstripe cards were a huge feat, but now their concept is relatively simple. The magnetic stripe on the back of the card is made up of extremely small magnets, which can be modified by a special device known as a solenoid. A solenoid is a coil of wire wound tightly into a helix, and when a current is passed through it, it is able to both write and read the tiny magnetic particles on the back of the card [10]. A magstripe card reader works in a similar fashion. When a card is swiped, the solenoid in the reader is charged and is able to read the information stored on it such as merchant ID, card number, expiration date, credit card limit, and card usage. With all of this information, the reader is able to process the transaction and the customer is on their way.

## Security Design of the MagStripe Credit Card

Since their inception in the ’60s, the security of magstripe cards is no longer sufficient for today’s day and age. Decades ago, technology wasn’t advanced enough for normal people to have a magstripe reader small enough for unwary customers to not notice, but today it is both cheap and extremely easy. The reason it is so easy is that the information on a magstripe card never changes from the day it is made to the day it is thrown away. And since the card doesn’t have a mind of its own and can’t tell the difference between a reader and a skimmer, anyone can skim and store the information and recreate an exact copy that no machine can tell the difference between. It was great for decades, but it is a major design flaw that cannot be fixed without a new type of card.

## Advancement of Security Attacks on MagStripe Cards

As the technology of a magstripe card became more widespread, its principal design flaws began to be taken advantage of. There have been countless data breaches where the security of magstripe cards is to blame. In September 2017, thieves were able to plant card skimmers in the self-checkout terminals at home depot [11]. Upon investigation, the same malware used in the massive 2013 Target data breach was found on the terminals. This software known as BlackPOS was used to aid in the breach that comprised roughly 40 million customers’ card information from Target.

## The Fall of the MagStripe Card

The magstripe card has served its time, but the fact of the matter is that its design and security was outdated years ago. There is no way to sufficiently improve its security either since its flaws come from its inherent design. Most information nowadays is encrypted and constantly changing making it a lot harder to steal, which leaves the static information of a magstripe card up for grabs for anyone with a cheap skimmer. The idea as a whole was a great success as it served nearly 60 years, but the sooner it is phased out the more money be kept out of malicious hands.

# innovation of emv chip cards

With the high amounts of credit card fraud building up in the world, the need for a newer and safer alternative also grew. The mid-1990s saw the production of the first implementation of chip cards in Europe which quickly spread to other parts around the world. In an effort to catch up with the rest of the world, the United States began introducing chip cards to the rest of the country in the 2010s. Its adoption has been slow compared to other countries, but it is still on the rise nonetheless. It is important to remember that EMV chip cards are not a new technology; however, they are relatively new to the United States.

## Security Design of the EMV Chip Credit Card

The process of an EMV chip card transaction has ten steps [8]:

1. Terminal and card chip make an application choice
2. Terminal reads data from that application
3. Data is authenticated offline to ensure that the card is not fraudulent
4. Transaction is confirmed
5. Card identity verification is done with CVM, PIN, or signature
6. Card reader checks floor limits
7. Terminal requests approval
8. Card approves
9. Online authorization request and authentication are completed and sent to the payment authorizer
10. Transaction is finalized

During an EMV transaction, a cryptogram is created using two-key triple DES cryptography [9]. The signature is generated from the most important data elements in either the optional online authorization step or the financial transaction step. This is the main security feature of the EMV chip card because it produces a unique cryptogram for each transaction, so if that data were to fall into the hands of an attacker, the information would only be good for that one singular transaction - nothing else could be bought with it.

During step three from above, the offline data authentication step (ODA), a cryptographic check to validate the card using public-key cryptography. There are typically two types of offline authentication depending on the card of the user: static data authentication (SDA) and dynamic data authentication (DDA) [9]. There is a third type called combined data authentication (CDA), but that is just another type of DDA. SDA is typically less secure than DDA because SDA only ensures that the data from the chip has not been manipulated since it has been issued, while DDA also ensures that the card is not a copy of the original card. The choice of which data authentication method to use is up to the card issuer and depends on cost per card and speed of transaction, so some card issuers are not willing to use DDA [9].

## The Rise of the EMV Chip Card

The rapid implementation of EMV chip cards happened at different times around the world. On one hand, Europe began its implementation of these chip cards in the 1990s due to the cost of phone line card authorization. America, however, began its adoption of these cards in the 2010s due to high profile data breaches [5]. This lag in response caused many credit card fraudsters to shift their efforts to the United States to take advantage of this lack of security. Why was the response so late? Comparatively to the rest of the world, the United States already had higher security measures when the chip cards were first released, so there was no high urgency to adopt these cards. As those security measures became outdated in the decades to come, the chip cards soon began to be seen as a necessity, so the United States was forced to catch up [6].

That being said, the United States still lags behind the rest of the world in the adoption of the chip card. In 2018, “53.5% of general-purpose U.S. card-present transactions were so-called chip-on-chip… up from 41.2% in 2017,” yet Europe is sitting at around 97.3% [3]. The chip card base grew up to 842 million in 2018, up 7.3% from the previous year, which accounted for a new adoption rate, the percentage of payment cards with an EMV to chip, that trails every major world region besides Asia [3].

*Adoption rates for world regions* [3]:

* Africa/Middle East: 87.8%
* Latin America: 86.9%
* Europe Zone 1: 85.5%
* Europe Zone 2: 80.4%
* United States: 60.7%
* Asia: 51.0%

If this trend persists, then the U.S. will catch up to the rest of the world average within the next few years.

# Proven security of emv chip cards

Since the adoption of the EMV chip cards, data shows that credit card fraud has dropped tremendously while fraudsters still do not have a way to break past the security produced by the unique cryptograms. With current computing trends, it is likely that EMV chip cards will be secure for years to come.

## Analyze Fraud Data From Before vs. After EMV Chip Cards

The data on fraud from before and after EMV chip cards were deployed is a significant accomplishment. In September 2019, Visa reported an 87% decline in credit card fraud since EMV chip cards were deployed [12]. And since stores are required to use chip readers, they are now financially responsible for any fraudulent transactions completed on a magstripe reader.

## Results of our MagStripe Demonstration

The results of our demonstration show how easily credit card fraud could be done using Magstripe cards because of its lack of security. A card reader was purchased off of Amazon for $15 and used to recover the credit card data held on a Magstripe card, through which that data could be used to create a duplicate card or just used for online purchases. These Magstripe card readers can be bought from many different vendors, in many different shapes and sizes. Some of which allow for placement of the card reader over other card readers, so the victim would have no idea their card was even swiped by a fraudulent source, such as an extra reader placed over the top of a gas station pump’s reader.

With just a top-level understanding of the structure through which data is held on Magstripe cards, all the information needed to subtly create a counterfeit card can easily be extracted. If the transaction was done with an EMV chip card, however, this could not have been done so easily. It would have taken an expert in the field to be able to take advantage of, rather than somebody who just researched the Magstripe card anatomy for a week beforehand.

## Remaining Vulnerabilities of EMV Chip Cards and Potential Solutions

Although EMV chip cards are significantly more secure than their magstripe counterparts, they still have some weaknesses that are being exploited. Firstly, as online transactions continue to make up an increasingly larger percentage of transactions, there remains no way to use a chip for these transactions. Even if a card has a chip, if someone knows the card number, expiration date, and security code, they can make an online payment with that card. Second, some cards use chip and signature verification rather than chip and pin verification. When a card is inserted into a reader, most readers will ask for a signature as a form of verification, but the truth is that signatures are not secure and can be easily replicated. An easy alternative is using a pin. This way a thief has to know an exact code in order to complete a transaction rather than just writing with a pen. Another simple flaw is that some stores will still make you swipe your cards magstripe instead of using the chip. Sometimes this is because it is broken for whatever reason, but whenever an EMV card is swiped, it is then susceptible to all the security problems of a magstripe card, which defeats the whole purpose of an EMV chip card.

# Conclusion

In conclusion, EMV chip cards are much more secure than their predecessor, the MagStripe card, for the main reason of utilizing cryptography to secure the card user’s payment information upon each transaction. This inclusion of the cryptography makes every transaction unique and gives the attacker no real information to work with once that transaction information is intercepted. Because of this, the United States will continue to see dramatic drops in credit card fraud once the shift to EMV chip cards has fully completed. However, malicious parties will also continue to innovate new ways to execute attacks on EMV cards, so the dynamic adaptability of online and electronic payment methods must continue to be improved for the sake of the general public.

# References

1. *Chip Card Security: Why is EMV More Secure?*, Square, 2019. Accessed on: Sept. 8, 2020. [Online]. Available: https://squareup.com/us/en/townsquare/why-are-chip-cards-more-secure-than-magnetic-stripe-cards
2. D. Gray, The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation’s Data Breach, ResearchGate, Feb. 2015. Accessed on: Sept. 8, 2020. [Online]. Available: https://www.researchgate.net/publication/276381800\_The\_Implementation\_of\_EMV\_Chip\_Card\_Technology\_to\_Improve\_Cyber\_Security\_Accelerates\_in\_the\_US\_Following\_Target\_Corporation's\_Data\_Breach
3. J. Olson, *A Brief History of EMV Technology*, FattMerchant, June 2017. Accessed on: Sept. 8, 2020. [Online]. Available: https://fattmerchant.com/blog/brief-history-emv-technology/#:~:text=EMV%20gets%20its%20name%20from,American%20Express%20to%20form%20EMVCo.
4. T. Groenfeldt, *US Credit Card Fraud is Spiking Ahead of EMV Secure Chip Introduction*, Forbes, Jul. 2014. Accessed on: Sept. 8, 2020. [Online]. Available: http://www.forbes.com/sites/tomgroenfeldt/2014/07/17/us-credit-card-fraud-is-spiking-ahead-of-emv-secure-chip-introduction/
5. J. MacDonald, T. Tompkins, *The History of Credit Cards*, creditcards.com, Jul. 2017, Accessed on: Oct. 18, 2020. [Online]. Available: https://www.creditcards.com/credit-card-news/history-of-credit-cards/
6. Available: https://www.investopedia.com/terms/e/emv.asp#:~:text=The%20EMV%20standard%20was%20first,Europe%20than%20in%20the%20U.S.
7. J. Daly, *Chip Cards Make Gains, but the U.S. Still Lags Most of the World in EMV* Adoption, Digital Transactions, June 19, 2019. Accessed on: Sept. 8 2020. [Online]. Available: https://www.digitaltransactions.net/chip-cards-make-gains-but-the-u-s-still-lags-most-of-the-world-in-emv-adoption/#:~:text=Home-,Chip%20Cards%20Make%20Gains%2C%20but%20the%20U.S.%20Still%20Lags%20Most,the%20World%20in%20EMV%20Adoption&text=In%20cards%2C%20the%20U.S.%20chip,60.7%25%20from%202017's%2058.5%25.
8. *How EMV Chip and PIN Technology Contributes to Security*, Sumup, 2019. Accessed on: Sept. 9 2020. [Online]. Available: https://sumup.com/emv-credit-card-chip/
9. *A Guide to EMV Chip Technology*, EMVCo, Nov. 2014. Accessed on: Oct. 12 2020. [Online]. Available: https://www.emvco.com/wp-content/uploads/2017/05/A\_Guide\_to\_EMV\_Chip\_Technology\_v2.0\_20141120122132753.pdf
10. Ashish, *Magnetic Strips: How Do Magnetic Strips on Credit Cards Work,* ScienceABC, Oct. 20 2019. Accessed on: Oct. 12 2020. [Online]. Available: https://www.scienceabc.com/innovation/how-magnetic-strips-stripes-tape-on-credit-room-key-cards-work.html
11. *In Home Depot Breach, Investigation Focuses on Self-Checkout Lanes,* KrebsonSecurity, Sept. 14 2018. Accessed on: Oct. 12 2020. [Online]. Available: https://krebsonsecurity.com/tag/target-data-breach/
12. *EMV Fraud: 5 Years Later*, ChargeBacks, Oct. 14 2020. Accessed on: Nov. 21 2020. [Online[. Available: https://chargebacks911.com/emv-fraud-5-years-later/