Practical Magnetic Stripe Security

by Jason Brown

California State Polytechnic University Pomona

2015

Table of Contents

What power is in a name?

For centuries, wars have been carried out “in the name” of kings, laws have been signed into effect with the names of government officials, and property has been owned under an individual’s name. Yet there is no intrinsic power to the words “Napoleon Bonaparte”, nor “George Washington”, nor “Steve Jobs”. Their power came not from their names, but what they represented.

In reality a person’s name is only a reflection of their identity. A person can take any name they like, but it does not change who they are. In the context of security, the question quickly becomes how a person’s identity can be verified, regardless of the information that they give.

Institutions seek to manage risk by verifying that individuals have the permission to perform specific actions. We can see this risk management played out in banks, which identify their customers in order to prevent theft, and secure facilities which verify that individuals have the right to access the premises, yet identity theft is arguably more of a problem today than it has ever been before.

The modern responses to identity verification range from highly technical biometric verification, to simple human verification, each with their own strengths and limitations. Various technologies assist in these methods of verification; keys permit holders access to locked areas, photo ID’s utilize visible identity clues, and fingerprints track detailed and unique biological data to confirm who a person is.

One of the most prevalent forms of modern identity verification is something that almost everyone carries with them at all times, yet very few understand on a technical or security level, namely Magnetic Stripe Cards. Credit cards, hotel keys, and even many identification cards all have magnetic stripes in them which contain information that can be read by a computer when swiped through a magnetic reader.

The use of magnetic stripe cards has become incredibly prevalent because of their low cost, user-friendly nature, and the widespread acceptance of magnetic reader technology. Magnetic stripe cards have become an incredibly convenient way for people to make payments and gain access to secure locations, but that does not mean consumers or security professionals should blindly trust this technology.

In this paper, an overall picture of the technology, security flaws, and proper security practices behind magnetic stripe cards will be explained in a way that both consumers and professionals can better understand, and more safely use, magnetic stripe cards as a method of identity verification.

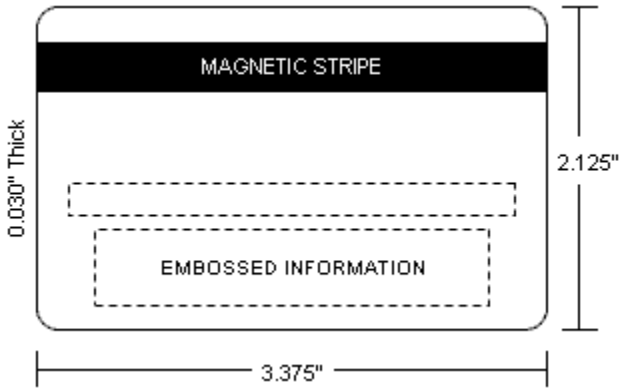
Magnetic Stripe Theory

Before we can understand how magnetic stripe cards work in a security situation, we must understand the physics behind them[1].

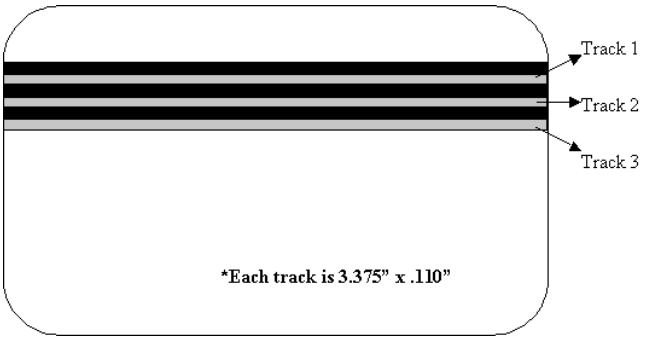
Magnetic stripe cards are the technological descendant of magnetic tape storage, the technology used in cassette tapes and early computer memory systems. They were initially designed by IBM engineer Forrest Parry in the early 1960's, when he attached a strip of magnetic tape to a plastic card as an identification tool for the CIA[2]. This tool quickly developed as a useful technology for the public in credit cards and identification cards, and remains relatively unchanged up to today.

With the widespread use of magnetic stripe cards, a method of standardization was required to make the technology easy to implement. The International Organization for Standardization[3] put forth a number of standards for the physical design of magnetic stripe cards, and the format of data to be used on them (See appendix A).

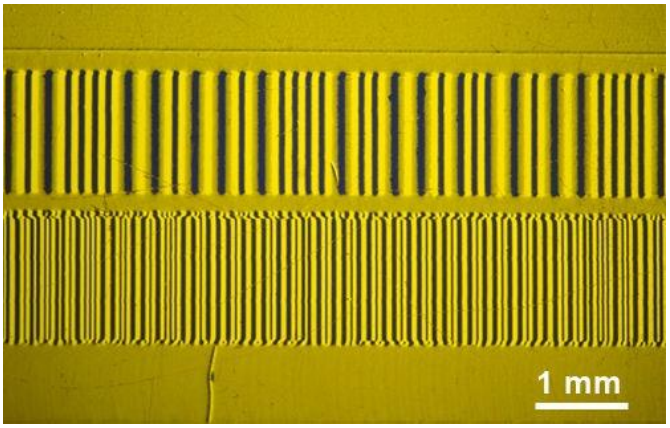
These standards dictate that a normal magnetic stripe card is a 3.375in by 2.125in by 0.030in plastic card, which may have images or data imprinted or embossed on its surface. Yet it is neither the card, nor the information printed on it that we are interested in. The information printed on the card is there for human reference, but significantly more information is stored on the "magnetic stripe" that the card gets its name from.



The magnetic stripe is a 0.330in section of the card made of a ferromagnetic material that is able to receive and hold data in the form of magnetic charge. Though we only see a single black stripe on the card, the data is actually stored in three separate lines, or "tracks".

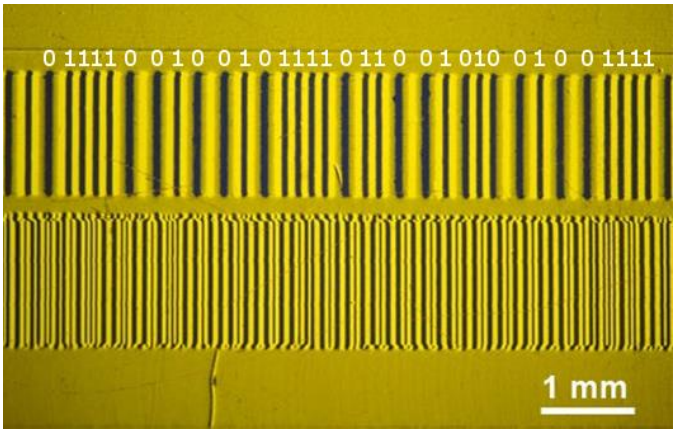


Each track stores slightly different data[4], but before we look at the actual data on the stripe, we should understand how it is stored there. Magnetic stripe technology utilizes the properties of ferromagnetic materials to hold a magnetic alignment even after being exposed to a magnetic field. In practice, this means that when in a strong enough magnetic field, the miniscule bits of the ferromagnetic strip will align themselves with the field (either positive to negative, or negative to positive). By controlling the fields with a magnetic stripe writer machine, intricate magnetic patterns can be imprinted on the stripe, in what looks like a visual representation of Morse code.



The image above depicts two tracks of a magnetic stripe, and shows the alignment of the ferromagnetic particles within each strip. In any one track, some of the aligned magnetic sections (shown as vertical black bars) have a width of either 1 unit or 2 units. The actual units of this width don't matter (you can see the second row is significantly more compact than the first) but the relationship between the two is important.

These bars are important because the information on a magnetic stripe is not written in letters and numbers, but in binary. The thick black bars represent a binary value of 0, while the thin bars represent a binary value of 1. Using a machine that can read the tiny magnetic flux fields that these bars give off, and translate it into binary, the message that a strip holds can begin to be understood.



All of this data is designed to be read by a computer, therefore to get a better picture of how the technology works, we will trace each step a computer takes to translate this information from a long string of binary to something we intuitively understand. Take for example, this credit card:

A standard financial card stores certain pieces of information on track 1 of the magnetic stripe, including the cardholder's name, the account number, the expiration date, and other discretionary data.

When the magnetic information of track 1 is read by a magnetic stripe card reader, the data is usually automatically translated from a binary string to a hexadecimal string, which is shorter, but just as easily understood by a computer.

Hexadecimal Data:

8B8A8D22750A96AF60CD8AE58AD42749F685EB3225653D1E16591F1933469
10204081020408102040810204081020408102040810

To understand this data, we need to first put it in a form that we can work with, namely binary. Translating from hexadecimal to binary is a relatively simple base conversion (base 16 to base 2), and automated translation can be found easily on the internet.

Binary Data:

100010111000101010001101001000100111010100001010100101101010111
111011000001100110110001010111001011000101011010100001001110100
100111111011010000101111010110011001000100101011001010011110100
011111000010111001011001000111111000110010011001101000110100100
010000001000000100000010000001000000100000010000001000000100000010
000001000000100000010000001000000100000010000001000000100000010000
10000001000000100000010000

Now translating from binary to something a human can understand takes a little more work. ISO specifications state that track 1 data is to be encoded in a 7 bit ALPHA data format. Though not every magnetic stripe card follows these guidelines, all financial cards do, simplifying this example.

To get readable data, the binary must be broken down into chunks of 7 bits (characters) each. A single chunk will correspond to a single character of our final data. The first chunk of this binary data is "1000101". This data can be translated using an automated program, or manually using a binary conversion table[5], such as those supplied in Appendix B, which contains much more detailed information on binary encoding and the different types of ISO encoding commonly used (7 bit ALPHA and 5 bit BCD formats).

To start this process, we take the first 7 bit chunk of binary, and convert it using a table (each chunk is read starting with the LEAST significant bit, AKA from right to left).

1010001 = %

The % symbol is called the "start sentinel", and tells the reader machine where to begin recording information. Here are a few more conversions using the next chunks to show how the remaining data is decoded:

0100011 = B
1000101 = 1
0100101 = 2
1100100 = 3
...
0000100 = 0
0000100 = 0
1111100 = ?

Filling in the rest of the conversion, the final data looks like this:

%B1234567898765432^HOLDER/CARD
^99120000000000 00000000000?

The data is finally in a human-friendly format, and details all the information that track 1 of a financial card should contain[6]. There is the account number, the cardholder name, the expiration date, and area for other discretionary data. All this data was contained in the magnetic stripe, ready to be read by anyone with the technology and skill to decode it!

There are many more important factors in the decoding of magnetic stripe data, such as unique binary encoding formats, variable magnetic data densities, and parity error checking, described in Appendix B, but this explanation gives a general overview of how data is stored on a card.

Basic Security Theory

Now that we have an understanding of how a magnetic stripe card holds data, we need to discuss its place as a modern security tool.

Security as whole is an incredibly dynamic and shifting industry, constantly changing as new threats appear, and old security is exploited. Yet the main concepts of effective security remain the same, no matter how technology changes. The constants of security include a security network which is used to protect assets from interference by increasing the risk, complexity, and cost of an attack[7].

In broad terms, a "security network" is all of the aspects of control that a security administrator uses to make sure that their assets are protected from interference. This definition of security can be applied to any number of situations, but we generally see it play out either in personal security, such as the protection of private property, or corporate security, which protects the information or assets of a group.

Theoretical security becomes a relatively simple matter when this definition is applied. If you bury $20 at an undisclosed location in the Arctic Circle, both the risk and complexity of an attack on this asset become enormous, and the cost of such an operation would far outweigh the reward.

In the real world though, theoretical security only serves as a starting point for practical security. In practice, a perfect security network is impossible, and so many more factors must be taken into account. Practical security often deals with high value assets that must both be protected, and easily accessed by trusted individuals. The goal behind practical security is still to increase risk, complexity, and cost for attackers, but only at a reasonable cost and margin of inconvenience for the security administrator. Practical security also has to deal with the ever-present issue of human error that propagates through networks with more members.

This disparity between theoretical security and practical security is why we can never describe an asset as perfectly secure, but we can observe stronger and weaker systems of security, and try to improve to the point where an attack is at the very least *unlikely* to succeed.

Magnetic stripe cards are not a security network by themselves, but they function as an important part of how many kinds of assets are protected. Magnetic stripe cards are classified as a "transferrable identity verification item", much like a key or a password, which serves as an object that confers specific permissions within a security network. These permissions often have to deal monetary transactions or secure physical access.

Technologies like magnetic stripe cards serve a very important role in practical security: *authentication*. The process of authentication is how individuals identify themselves to a security network, just like an individual's name is how they identify themselves to others. In fact, transferrable identity verification items function in much the same way that names do, though they tend to be much less accessible, and thus harder to duplicate.

Finally, once an individual is authenticated to a network, they are *authorized* to perform specific actions within the network. Authorization refers to the specific permissions that an authenticated individual is allowed to complete. This prevents individuals from abusing their power within a network, even if their identity is known.

All of these concepts may seem vague and theoretical, and it can sometimes be hard to see how they play out in a practical situation. A tangible example of how magnetic stripe cards can be used in a security network is the practice of using keycards to keep an important facility safe.

When a security administrator decides to use magnetic key cards as a means of limiting access to a facility, they begin by designing a network around access obstacles. Access obstacles, such as doors, gates, and windows, are designed to keep intruders out, while still maintaining functionality for authorized users. The distinction between authorized users and unauthorized intruders is made by a pairing of an authentication control unit (in this case a magnetic stripe card reader), and a transferable identity verification item (in this case a magnetic stripe card).

The access obstacles and authentication control units create an access control system, which is the backbone of any secure facility. The security administrator may then add supplemental security features, such as monitoring cameras or security guards to further prevent tampering and protect the network.

Magnetic Stripe Risk & Reward

Now that we understand how magnetic stripe cards work, and the role that they play in a security network, we can discuss their strengths and weaknesses as a security tool.

In practical security, cost and ease of use are two major factors to a successful security network. Because of their relatively simple materials and construction, and the widespread standardization of reader technology, magnetic stripe cards tend to be both very cheap, and easy to utilize.

The price of a plastic card with ferromagnetic material is very low, often less expensive than even a key. The cost of card readers and writers used to be a prohibitive expense for small business or consumer use, but as the technology has developed, the price of these machines has decreased significantly. Secure access with magnetic stripe cards can now be set up quickly, and at a low price.

Another benefit of magnetic stripe technology is that it is already widely understood by the common consumer. While not very many people understand how data is stored on the card, or the physical specifications of these cards, most people understand the basic function: swipe your card to open a door or pay a bill. Using magnetic stripe technology does not require any special skills, and therefore the cost of employee training is greatly reduced, and there are fewer user-error problems that occur.

Magnetic stripe cards offer one particularly important feature that makes them beneficial for modern security networks; authentication with this technology is incredibly dynamic. Systems that use standard locks must be completely overhauled every time there is a lost or stolen key, if they want to remain completely safe. Magnetic stripe cards, on the other hand, can simply be re-magnetized with new data, and the reader technology can be reprogrammed without replacement. A lost card is much less devastating than a lost key, as long as the security breach is properly addressed.

The customization of magnetic stripe systems is also a benefit, though not as unique as its dynamic differentiation. Data on the cards, much like a password, is unique to the individual user, and therefore authorization is much more customizable. It is simple to assign individuals permission to certain tasks, and limit their involvement in others, while a technology like physical keys quickly becomes too complex when you go much beyond a few levels of permission. Magnetic stripe data can also be tracked, creating a usage log that can be useful in identifying security breaches after the fact.

While there are many benefits to using magnetic stripe technology in a security network, it is more important to understand the weak points it can create. This security tool has some of the same flaws as other authentication systems, and a few issues unique to itself.

One of the primary flaws in magnetic stripe security is the ease and undetectably of a security breach through the unauthorized copying of cards. As we have discussed previously, the unique identifying aspect of a magnetic stripe card is the data that is stored on it; the actual plastic card that contains the data is not at all important in the authentication process. Because of

the standardized nature of the cards, any properly sized piece of plastic that contains the same data can be used in a system. This means that if the data on a card is somehow stolen, the actual card becomes irrelevant, and security can be circumnavigated by anyone with their own magnetic stripe writer.

Interestingly enough, the method of encoding used on the card does not in any way inhibit straight copying. Even if a proprietary encoding scheme is used, the raw magnetic data from the card can be copied from one card to another, though the data may be unintelligible to the naked eye unless the encoding is cracked.

On top of this, because of the nature of magnetic stripe cards, stealing the data on the card is as simple as a swipe. If a card is left unattended, the data on it can be recorded in seconds, without the owner's knowledge. A security breach such as this is especially dangerous because, left undetected, a security network is permanently compromised.

This type of flaw has wreaked havoc in the past through the illegal use of card skimmers that have stolen magnetic stripe data from ATMs across the country. By installing a miniature card reader into an ATM, on top of the machine's legitimate reader, criminals have been able to undetectably take data from people using the machine for financial transactions. This data can then be harvested, and used to impersonate the actual owners of the cards.

Though not as apparent as attacking the card data itself, card readers are another possible weak point in the system[8]. While not the focus of magnetic stripe security, it is important to consider safeguards to prevent tampering with the actual reading equipment. It is theoretically possible to electronically bypass a card reader for systems such as door locks, though this is typically harder and more obvious than attacking the system through the card data.

Finally, one of the largest risks when dealing with magnetic stripe security systems is the issue of data cracking. As previously discussed, most magnetic stripe cards use either 5 Bit Parity Code or ALPHA 7 Bit Parity Code. Since the translation from either of these types of binary to a form readable to the naked eye is already known, it is possible to replicate the information on the card. If there are enough samples of card data, it is even possible to crack the overall data scheme that the card uses.

Using the same sample data that we previously looked at, we can get a better understanding of how data cracking works:

%B1234567898765432^HOLDER/CARD
^99120000000000 000000000000?

Since we already have the data separated by category, we can easily replace each field with the data of another user. For example, if you somehow got a picture of John Smith's credit card, and knew his account number was 9876543212345678, and his expiration date was 7019, we could create a card identical to his, without ever swiping it. The data on this cracked card would look like this:

%B9876543212345678^SMITH/JOHN

^70190000000000 000000000000?

Obviously, credit card issuers do not make it this simple to crack their cards. The blue numbers, in our example all zeros, are proprietary information; usually a random assortment of numbers that are known by the card issuers that prevent simple spoofing of cracked data formats. Without this proprietary information though, magnetic stripe data can be easily replicated by anyone who can see a card long enough to memorize the numbers on it.

Clearly there are significant risks associated with the use of magnetic stripe security systems, but there are risks inherent to any type of security we seek to employ. There are also many definite advantages to this type of security, and therefore we must carefully assess if it is the right tool for the situation that we are trying to solve, and if so we must employ security measures to ensure that our magnetic stripe cards are as safe as possible.

Practical Magnetic Stripe Security

Security administrators use many different methods to ensure that their security networks are as safe as possible, and magnetic stripe systems are no exception. Once we understand the risks and rewards associated with a magnetic stripe card security system, we must seek to employ security measures that minimize the security risks that go along with using the technology.

As we discussed in the last section, the two primary security flaws intrinsic to magnetic stripe cards are the vulnerabilities to cracking and copying. There are quite a few different security measures already in use that prevent or discourage exploitation in these areas.

One security measure that we see, primarily in financial cards, is the use of proprietary information to prevent the cracking of card data. This string of data on the card is important because it is not at all related to the user of the card. Name, account number, and expiration date are all pieces of data that can be stolen simply by looking at the card, but proprietary data can only be read directly from the card's magnetic stripe. This means that, even if someone cracks the data structure of a card, and knows the account information of the person they wish to impersonate, they still do not have enough information to replicate that person's card.

The other security measure used to inhibit cracking is the use of unique data formats to encode information on cards. Most cards use ALPHA 7 BPC or 5 BPC encoding to translate user data into binary to be stored on the card. These formats are useful in that they are easy to read, but this standardization can also make it easier to crack. A security administrator could invent their own form of encoding, making it much more difficult to crack, without affecting how the authentication process works (because card readers can compare a card's binary to its authentication database, without converting to an unencoded format). Financial cards do not use unique data formats, but some other security cards use proprietary formats to obfuscate data. In especially sensitive situations, encryption could even be incorporated into the encoding to increase security.

Cracking can be a significant security risk to unprepared networks, but copying can at times be even harder to stop and detect. One security measure that inhibits card copying is the inclusion of verification codes that are not stored on the magnetic stripe, which are used to verify a user's authenticity. Verification codes are essentially inverse proprietary data; even if a card is swiped and the magnetic stripe data is stolen, there is a number on the actual card that must be known to use the data. This type of security measure is seen on financial cards, and is mostly used to prevent unauthorized online transactions. Credit card PINs also fall into the category of verification codes, but are not printed on the card to make them even more difficult to steal.

A security measure that is not often taken into account is the employment of an expiration system that deals with the possibility of long-term data theft. Because it is so hard to prevent the actual copying of magnetic stripe cards, occasional card expiration and reissuing can eliminate some security breaches that have already taken place. While not an incredibly secure measure, card expiration should be a part of every magnetic stripe security system, and should take place more often in more sensitive security networks.

The only way to truly counteract card copying and unauthorized access is by monitoring magnetic stripe card usage within a network. While not preventative, the reactionary security measure of usage monitoring is able to identify possible security breaches caused by data theft. Financial institutions strictly monitor purchases made with their cards in order to prevent unauthorized use; for example if a card issuer notices purchases made in two separate countries on the same day, they quickly become suspicious of the legitimacy of such purchases. These kinds of security measures can be employed in any network, and while they can be difficult and time consuming to utilize properly, pattern recognition and data monitoring can be incredibly effective.

I would also like to propose another security measure that is not currently in use that would significantly increase practical magnetic stripe security by giving a unique identity to each individual card in circulation. As mentioned in Appendix B, track 3 on magnetic stripe cards was designed to store transient magnetic data, such as the last purchase made with the card, which would change every time it was used. This data track fell out of use, partially because of the prevalence of data tracking, which has some of the same function of track 3 verification. By writing unique data to track 3 every use, and verifying it at the next use, the unique identity of each individual card can be maintained. If someone tries to copy a card, and use it, then there would be a disparity between the track 3 data on the two cards, which could be detected by the system. Track 3 verification would require more specialized reader/writer technology to function properly, but could work well in systems where usage monitoring is not as viable.

Finally, when considering magnetic stripe technology, it would be imprudent to not mention other similar technologies which are becoming prevalent in the security industry. Because magnetic stripe cards have not changed much in nearly 40 years, other types of authentication cards are starting to become viable alternatives, and they offer some security features that magnetic stripe cards cannot.

The most important challenger to mention is the quickly rising Smart Card technology[9]. Smart cards look a lot like magnetic stripe cards, but instead of storing data on a ferromagnetic stripe, they use embedded memory or microcontrollers to store or even process data within the card itself. Smart cards come in many flavors; some have external pin contacts which connect the

embedded circuitry to their readers, while others use radio-frequency identification (RFID) or near field communication (NFC) to transmit data without contact. Some cards merely store data like a magnetic stripe, while others have the processing power to perform onboard data protection and other security features. This technology has a much greater security potential than magnetic stripe cards, though it does have its own security flaws as well. Financial card issuers are beginning to incorporate smart-card technology into their magnetic stripe cards, and though it is currently not nearly as cost-effective or standardized as magnetic stripe cards, it is likely we will see smart card technology use increase in the years to come.

Conclusion

It is clear magnetic stripe security is on the decline; the push for more secure cards and biometric identity verification will inevitably oust magnetic stripe cards as the most secure form of authentication. This does not take away from the fact that magnetic stripe systems are a convenient, cheap, and understood type of security that is still incredibly relevant today. Magnetic stripe cards are among the top three identity verification tools used today, along with keys and passwords, and are likely to remain in their position for some time to come.

Hopefully after reading this, you have a better understanding of how magnetic stripe cards fit into modern security situations, whether you are a security professional seeking to utilize them in your network, a researcher looking to develop new security technology, or a consumer interested in keeping your own data safe. For those interested in learning more about magnetic stripe security, the appendices of this paper hold a wealth of practical information, and the bibliography contains references to many more specialized works on magnetic stripe technology.

It is important to remember, that with great knowledge comes great responsibility. I feel the need to specify, in case you haven't already realized, that it is a *bad idea* to use this information on magnetic stripe cards for shady business. By giving you the details on how to protect yourself in a world of magstripe cards, I have also given you the tools to exploit them. *Do not* copy cards that you do not have permission to copy, *do not* erase your friend's ID card as a prank, and *do not* mess with credit card fraud. You will more than likely be caught, because banks are most definitely smarter than you.

I would like to give a special thanks to "oooOO Count Zero OOooo", the author of "A Day in the Life of a Flux Reversal". His guide (published in 1992 mind you) is still one of the most clearly and well written papers on magnetic stripe technology on the internet. It inspired me to write a paper on this topic geared towards security professionals, while still maintaining information on many of the technical details that make magnetic stripe cards what they are today.

Finally I would like to thank you for taking the time to learn more about security! A society that understands security in general helps keep individuals from abusing the system, and that seems like a good thing in my book. I would welcome any further comments, questions, or criticisms at jbrownfisher@gmail.com.

Appendix A: ISO Standards

This section contains a brief overview of many ISO Standards pertaining to magnetic stripe cards, and a link to the full documents. These documents set forward standards that allow magnetic stripe cards to be easily used with standardized reader technology, instead of a proprietary reader being required for each type of card.

The following is information taken from the International Organization for Standardization[2] website.

ISO/IEC 7810

ISO/IEC 7810:2003 is one of a series of standards describing the characteristics of identification cards. It is the purpose of ISO/IEC 7810:2003 to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements.

ISO/IEC 7810:2003 specifies:

- four different sizes of identification cards with a nominal thickness of 0,76 mm and dimensions of:
  - ID-000 25 mm x 15 mm,
  - ID-1 85.60 mm x 53.98 mm,
  - ID-2 105 mm x 74 mm,
  - ID-3 125 mm x 88 mm;
- the conditions for conformance;
- the dimensions and tolerances of the identification cards;
- the construction and materials of the identification cards; and
- the physical characteristics of the cards such as bending stiffness, flammability, toxicity, resistance to chemicals, dimensional stability, adhesion or blocking, warpage, resistance to heat, surface distortions, and contamination.

ISO/IEC 7810:2003, together with a standard for test methods, provides for interchange between various types of identification card processing devices and systems.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31432

ISO/IEC 7811

ISO/IEC 7811-1

ISO/IEC 7811-1:2014 is one of a series of International Standards describing the parameters for identification cards as defined in the definitions clause and the use of such cards for international interchange.

It specifies requirements for embossed characters on identification cards. The embossed characters are intended for transfer of data either by use of imprinters or by visual or machine reading. It takes into consideration both human and machine aspects and states minimum requirements.

It is the purpose of ISO/IEC 7811-1:2014 to provide criteria to which cards shall perform. No consideration is given to the amount of use, if any, experienced by the card prior to test. Failure to conform to specified criteria should be negotiated between the involved parties.

ISO/IEC 10373 1 specifies the test procedures used to check cards against the parameters specified in ISO/IEC 7811-1:2014.

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=61935

ISO/IEC 7811-2

ISO/IEC 7811-2:2014 specifies requirements for a low coercivity magnetic stripe (including any protective overlay) on an identification card, the encoding technique and coded character sets. It takes into consideration both human and machine aspects and states minimum requirements.

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=61936

ISO/IEC 7811-6

ISO/IEC 7811 defines the characteristics of identification cards. ISO/IEC 7811-6:2008 provides criteria to which cards shall perform and specifies the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements.

ISO/IEC 7811-6:2008 specifies requirements for a high coercivity magnetic stripe (including any protective overlay) on an identification card, the encoding technique and coded character sets. It includes a modified algorithm for waveform measurement which produces more consistent results (incorporated from ISO/IEC 7811-6:2001/Amd.1:2005), and an additional requirement has been added for signal amplitude.

ISO/IEC 7811-6:2008 specifies the following:

- the conditions for conformance;
- physical characteristics for the card (warpage and surface distortions) and the magnetic stripe area (location, height and surface profile, roughness, adhesion, wear, and resistance to chemicals);
- the signal amplitude performance characteristics of the magnetic stripe;
- the encoding specification including technique (F2F), angle of recording, bit density, flux transition spacing variation, and signal amplitude;
- the data structure including track format, the use of error correction techniques;
- the location of encoded tracks.

ISO/IEC 7811-6:2008, together with a standard for test methods, provides for interchange between various types of identification card processing devices and systems.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50370

ISO/IEC 7811-7

ISO/IEC 7811-7(2004) is one of a series of International Standards describing the characteristics of identification cards. It is the purpose of ISO/IEC 7811-7 to provide criteria to which cards shall perform and to specify the requirements for such cards used for international interchange. It takes into consideration both human and machine aspects and states minimum requirements.

ISO/IEC 7811-7 specifies requirements for a high coercivity magnetic stripe (including any protective overlay) on an identification card, the encoding technique and coded character sets. This encoding technique provides for a card capacity of approximately 10 times that of a card conforming to ISO/IEC 7811-6. The number of tracks has been increased to six, each track being approximately half the width of tracks conforming to ISO/IEC 7811-6, located so that readers designed to read these high density tracks will also be able to read cards conforming to ISO/IEC 7811-2 and ISO/IEC 7811-6. Data is encoded in eight-bit bytes using the MFM encoding technique. Data framing is used to limit error propagation, and error correction techniques further improve reliability of reading.

ISO/IEC 7811-7 specifies:

- the conditions for conformance,
- physical characteristics for the card (warpage and surface distortions) and the magnetic stripe area (location, height and surface profile, roughness, adhesion, wear and resistance to chemicals),
- the signal amplitude performance characteristics of the magnetic stripe,
- the encoding specification including technique (MFM), angle of recording, bit density, flux transition spacing variation and signal amplitude,
- the data structure including track format, use of error correction techniques, user data capacity for ID-1, ID-2 and ID-3 size cards, and decoding techniques, and
- the location of encoded tracks.

ISO/IEC 7811-7, together with a standard for test methods, provides for interchange between various types of identification card processing devices and systems.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34382

ISO/IEC 7811-9

ISO/IEC 7811 defines the characteristics of identification cards. ISO/IEC 7811-9:2008 specifies the physical characteristics of a tactile identifier mark used by visually-impaired card holders to distinguish their cards. It defines the area on the card for the tactile identifier mark (TIM) and the layout of Braille style embossed dots arranged in patterns to enable easy tactile recognition.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46200

ISO/IEC 7812

ISO/IEC 2012-1

ISO/IEC 7812-1:2006 specifies a numbering system for the identification of issuers of cards that require an issuer identification number to operate in international, interindustry and/or intra-industry interchange.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39698

ISO/IEC 7813

ISO/IEC 7813:2006 specifies the data structure and data content of magnetic tracks 1 and 2, which are used to initiate financial transactions. It takes into consideration both human and physical aspects and states minimum requirements of conformity. It references layout, recording techniques, numbering systems, registration procedures, but not security requirements.

ISO/IEC 10373 specifies the test procedures used to check ID-1 cards against the parameters specified in ISO/IEC 7813:2006.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43317

ISO/IEC 8583

ISO/IEC 8583-1

ISO 8583-1:2003 specifies a common interface by which financial transaction card originated messages may be interchanged between acquirers and card issuers.

It specifies message structure, format and content, data elements and values for data elements. The method by which settlement takes place is not within the scope of this part of ISO 8583.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31628

ISO/IEC 8583-3

ISO 8583-3:2003 establishes the role of the maintenance agency (MA) and specifies the procedures for adding messages and data elements to ISO 8583-1 and to codes listed in Annex A of ISO 8583-1.

The responsibilities of the MA relate to all message type identifiers and classes, data elements and sub-elements, dataset identifiers and codes within ISO 8583-1, with the exception of Institution Identification Codes.

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35363

ISO/IEC 4909

ISO/IEC 4909:2006 establishes specifications for financial transaction cards using track 3 and is intended to permit interchange based on the use of magnetic stripe encoded information. It specifies the data content and physical location of read/write information on track 3 and is to be used in conjunction with the relevant parts of ISO/IEC 7811 and ISO/IEC 7812.

ISO/IEC 4909:2006 recognizes the need for formats of track 3 which can be used independently of, or in conjunction with, track 2 as defined in ISO/IEC 7813. This approach is intended to permit the greatest degree of flexibility within the financial community in facilitating international interchange.

Using track 3 in conjunction with track 2 is a mode of operation in both on-line and off-line interchange environments. This mode of operation requires that the original encoded data on track 2 be read; the data on track 3 be read; and, if update is required, all the data on track 3 be rewritten.

Independent use of track 3 is an alternative mode of operation permitting both on-line interchange and off-line interchange based on mutual agreement between interested parties. It requires reading only of the data on track 3 and, if update is required, the rewriting of all the data on track 3.

http://www.iso.org/iso/catalogue_detail.htm?csnumber=43309&ei=_kizUabZDvfi4AO9_IDAAQ&usg=AFQjCNHwqVa43v1NX_L9Tm5OlvuqRPZ2YA&sig2=X-RjSmISXB6cMP3k7wtlvA

ISO/IEC 10373

ISO/IEC 10373-2

ISO/IEC 10373-2:2006 defines test methods for the magnetic recording characteristics of identification cards according to the definitions given in base standards ISO/IEC 7811-2, ISO/IEC 7811-6 and ISO/IEC 7811-7.

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=240&ics3=15&csnumber=39497

Appendix B: Binary Conversion Tables and More

The subjects of binary conversion, parity, coercivity, and magnetic density are incredibly complex, and not necessarily important for the majority of consumers or professionals seeking to securely use magnetic stripe cards. This section contains information for those who want an even more detailed understanding of the physics behind magnetic stripe cards, or the encoding techniques that they use.

Binary Conversion Tables

The two ISO standardized binary formats for magnetic stripe cards are the Binary Coded Decimal 5 BPC and ALPHA 7 BPC (BPC = bit parity code). The difference is that 5BPC uses 5 bit chunks of binary, but can only express numbers (and a few control characters), while 7BPC can express both numbers and letters. In general, track 1 uses 7BPC, while tracks 2 and 3 use 5BPC (though track 3 usually not used at all).

Remember, these data formats are only standards, and not every card will conform to them (computers can verify data without translating them out of binary, these conversions are technically only compensating for human interaction).

IMPORTANT: “Bit 1” is the LEAST significant bit. Once you have a chunk of 5 or 7 bits, Bit 1 is the farthest one to the right, so read the chunk backwards for these tables.

5 Bit Parity Code

Bit 1	Bit 2	Bit 3	Bit 4	Parity Bit 5	Character	
0	0	0	0	1	0	
1	0	0	0	0	1	
0	1	0	0	0	2	
1	1	0	0	1	3	
0	0	1	0	0	4	
1	0	1	0	1	5	
0	1	1	0	1	6	
1	1	1	0	0	7	
0	0	0	1	0	8	
1	0	0	1	1	9	
1	1	0	1	0	;	Start Sentinel
1	0	1	1	0	=	Field Separator
1	1	1	1	1	?	End Sentinel
0	1	0	1	1	:	Control
0	0	1	1	1	<	Control
0	1	1	1	0	>	Control

ALPHA 7 Bit Parity Code

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Parity Bit 7	Character	
0	0	0	0	0	0	1	space	
1	0	0	0	0	0	0	!	
0	1	0	0	0	0	0	"	
1	1	0	0	0	0	1	#	
0	0	1	0	0	0	0	$	
1	0	1	0	0	0	1	%	Start Sentinel
0	1	1	0	0	0	1	&	
1	1	1	0	0	0	0	'	
0	0	0	1	0	0	0	(	
1	0	0	1	0	0	1	)	
0	1	0	1	0	0	1	*	
1	1	0	1	0	0	0	+	
0	0	1	1	0	0	1	,	
1	0	1	1	0	0	0	-	
0	1	1	1	0	0	0	.	
1	1	1	1	0	0	1	/	
0	0	0	0	1	0	0	0	
1	0	0	0	1	0	1	1	
0	1	0	0	1	0	1	2	
1	1	0	0	1	0	0	3	
0	0	1	0	1	0	1	4	
1	0	1	0	1	0	0	5	
0	1	1	0	1	0	0	6	
1	1	1	0	1	0	1	7	
0	0	0	1	1	0	1	8	
1	0	0	1	1	0	0	9	
0	1	0	1	1	0	0	:	
1	1	0	1	1	0	1	;	
0	0	1	1	1	0	0	<	
1	0	1	1	1	0	1	=	
0	1	1	1	1	0	1	>	
1	1	1	1	1	0	0	?	End Sentinel
0	0	0	0	0	1	0	@	
1	0	0	0	0	1	1	A	
0	1	0	0	0	1	1	B	
1	1	0	0	0	1	0	C	
0	0	1	0	0	1	1	D	
1	0	1	0	0	1	0	E	

Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Parity Bit 7	Character	
0	1	1	0	0	1	0	F	
1	1	1	0	0	1	1	G	
0	0	0	1	0	1	1	H	
1	0	0	1	0	1	0	I	
0	1	0	1	0	1	0	J	
1	1	0	1	0	1	1	K	
0	0	1	1	0	1	0	L	
1	0	1	1	0	1	1	M	
0	1	1	1	0	1	1	N	
1	1	1	1	0	1	0	O	
0	0	0	0	1	1	1	P	
1	0	0	0	1	1	0	Q	
0	1	0	0	1	1	0	R	
1	1	0	0	1	1	1	S	
0	0	1	0	1	1	0	T	
1	0	1	0	1	1	1	U	
0	1	1	0	1	1	1	V	
1	1	1	0	1	1	0	W	
0	0	0	1	1	1	0	X	
1	0	0	1	1	1	1	Y	
0	1	0	1	1	1	1	Z	
1	1	0	1	1	1	0	[	
0	0	1	1	1	1	1	\	
1	0	1	1	1	1	0	]	
0	1	1	1	1	1	0	^	Field Separator
1	1	1	1	1	1	1	_	

Parity Error Checking

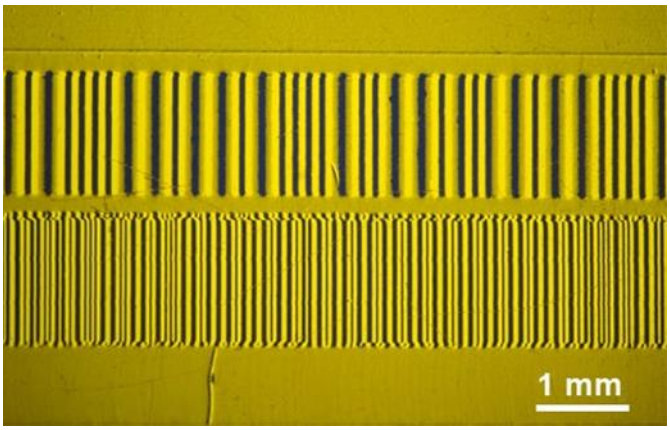
In each of the binary tables above, you can see that there is a column labelled “Parity”. The parity bit in each chunk is used as a method of error checking, so that reader equipment knows if there was some kind of error reading the binary off the card. ISO standards dictate that 5BPC and 7BPC use odd parity, therefore the last bit in any chunk should make the sum of the bits in the chunk odd.

For example, in the 7BPC representation of “W”, 1110110, the sum of the first six bits is 1 + 1 + 1 + 0 + 1 + 1 = 5. Since five is odd, the chunk is already odd, and the parity bit will be 0. On the other hand, in the 5BPC representation of “3”, 11001, the sum of the first four bits is 1 + 1 + 0 + 0 = 2. Since two is even, the parity bit will be 1 to make the chunk odd.

It is also important to note that after the end sentinel on a magnetic stripe comes the Longitudinal Redundancy Check, which is a final parity check to verify the read data. Most card readers do not show this data, but it is used catch possible errors in the first parity check.

Magnetic Density

Remember, a magnetic card reader doesn't look at the width of each individual magnetic section, but the relationship between the strips. For example:



The second row of magnetic data has smaller strips, but they still have a 2:1 ratio of wide and thin strips. This compression of magnetic strips is called "Magnetic Bit Density". In general, based on ISO standards, tracks 1 and 3 have a high bit density of 210 bits per inch, while track 2 has a bit density of 75bpi.

It is also good to note that track 3 was designed to store transient magnetic data (AKA it was meant to record the last purchase made with a card, for verification purposes), but the use of track 3 has greatly declined, and it is rarely used in practical applications.

Coercivity

The coercivity of a magnetic card has to do with the ferromagnetic material used in its construction, and what strength of magnetic field is needed to alter the data on the stripe. This attribute is important so that light environmental magnetic fields (such as those a cell phone give off) do not wipe the data on a card, but the data can still be altered by stronger magnetic fields.

ISO standards define two different coercivities for magnetic stripe cards. Low coercivity cards have a rating of around 300 Oersteds, while high coercivity cards have a rating of about 4000 Oersteds. These values represent the strength of magnetic field required to change the data on the stripe.

The majority of publicly available cards are low coercivity, and short of placing them on top of an electric motor or rubbing them with magnets you have laying around, they should stand up to most environmental magnetism. High coercivity cards tend to show up in ID cards that need to be more robust, or need to operate in areas that may have some kind of extreme environmental magnetic exposure.

Appendix C: Assorted Magnetic Stripe Data

For those looking for a more tangible example of various types magnetic stripe data, I am including a list of the data contained on many of the cards I read while I was doing research for this paper. Data marked with a "*" has been changed to protect personal information, but all effort has been put into maintaining data formats for educational purposes.

Apartment Access Keycards:

> These cards use a proprietary encoding scheme which I could not crack. From observation, I assume it is some type of 5 bit code, but it is not 5BPC.
>
> Card 1 (Raw)
> Track 1 - No Data
> Track 2 - No Data
> Track 3 - ECD3F0D86DD5C713CBD1546A346824
>
> Card 2 (Raw)
> Track 1 - No Data
> Track 2 - No Data
> Track 3 - ECE7A494ED14DE5782CD49A034B8C4

Student ID Cards:

> These two cards use standard track 2 encoding, which is 5BPC. As far as I can tell, the data to the left of the separator is proprietary data, and the data to the right is an identification number.
>
> Card 1 (Raw)
> Track 1 - No Data
> Track 2 - D0439409B0AA210B0601809AD0D7F6
> Track 3 - No Data
>
> Card 1 (Decoded)
> Track 1 - No Data
> Track 2 (5BPC) - 00328615211=010186605
> Track 3 - No Data
>
> Card 2* (Raw)
> Track 1 - No Data
> Track 2 - D04394732426610B06010C021693E7
> Track 3 - No Data
>
> Card 2* (Decoded)
> Track 1 - No Data
> Track 2 (5BPC) - 00327344311=010010064
> Track 3 - No Data

Gift Cards:

This assortment of gift cards all use standard track encoding of either 5 or 7 BPC. Since they are not linked to an account, most of the data is just proprietary data.

Card 1 (Raw)
Track 1 - A28DA649856A542A346F51B52A754AF91C3779DB8102040810204081020
4081020408102040817D146C54B162841BD727C02
Track 2 - D3733256A410B82AD788B405044201AF09CE4210FA
Track 3 - No Data

Card 1 (Decoded)
Track 1 (7BPC) - B639455488785572^BANSV^1812110873
Track 2 (5BPC) - 639455488785572=181211057477111
Track 3 - No Data

Card 2 (Raw)
Track 1 - A39F2161D88757541F1070FF2180
Track 2 - D420440459093F60
Track 3 - No Data

Card 2 (Decoded)
Track 1 (7BPC) - S3TXCXUJPCPP
Track 2 (5BPC) - 114208304
Track 3 - No Data

These next two cards are unique in that the data on the magnetic stripe is identical to the card number printed on the back. This type of card could be copied by simply looking at the back of a card and translating it to binary. These unsecure cards come from two separate major retailers.

Card 3 (Raw)
Track 1 - No Data
Track 2 - D34396A0504349599390E67956FD
Track 3 - No Data

Card 3 (Decoded)
Track 1 - No Data
Track 2 (5BPC) - 60362812645947173756
Track 3 - No Data

Card 4 (Raw)
Track 1 - No Data
Track 2 - D42A144028271150C33FE0
Track 3 - No Data

Card 4 (Decoded)
Track 1 - No Data
Track 2 (5BPC) - 15021024725013
Track 3 - No Data

Appendix D: Glossary of Terms

Some of the terms in this paper have either been appropriated or invented for the purpose of clarity. Herein lies a list of how I personally intended for the terms to be defined.

5 BPC – "5 Bit Parity Code". A type of encoding used to store data that has only numbers; contains parity error checking. See Appendix B.

(ALPHA) 7 BPC – "Alphanumeric 7 Bit Parity Code". A type of encoding used to store data that has both letters and numbers; contains parity error checking. See Appendix B.

Access Control System – A set of security tools used to authenticate an individual, and then give them authorization to parts of the security network; in the case of magnetic stripe cards the authentication control system is made up of an access obstacle (door, ATM, etc.), an authorization tool (card reader), and a transferable identity verification tool (magnetic stripe card).

Authentication – The process of verifying an individual's identity within a security network; in general used to give that person authorization to perform tasks within the network.

Authorization – An individual's permissions within a security network.

BCD – "Binary Coded Decimal". A decimal value expressed by binary chunks rather than a binary value.

Binary – A base 2 number system where information is made up of only two values, 1 and 0; the standard and most basic form of digital communication.

Bit – The smallest part of binary data; a single binary character.

Chunk – A section of data; in general a section of binary data that corresponds to a single character of information.

Coercivity – A measurement of a ferromagnetic material's resistance to change; measures the strength of field necessary to change the magnetic alignment of a track. See Appendix B.

Contact Cards – A type of authentication card that must touch its reader to transmit information.

Copying – The process of replicating data by gaining access to the data.

Cracking – The process of replicating data without actually ever having access to that specific data through understanding of data formats and knowledge of personal information.

Decoding – The process of translating data from its encoded format back to its original format; in general translating data from something easy to store electronically to a human-readable format.

Discretionary Data – See "Proprietary Information".

Encoding – The process of translating data from one format to another; in general translating data from a human-readable format to something easier to store electronically.

Ferromagnetic Material – A material, such as iron, which holds a magnetic alignment that persists even after being exposed to a magnetic field.

Hexadecimal – A base 16 number system; an easy way to condense binary data into a shorter string of information.

ISO – "International Organization of Standardization" (Yes, the letters are out of order).

Longitudinal Redundancy Check – A type of error-detection that performs a final check on parity data in order to prevent double-error situations.

Magnetic Alignment – When magnetic particles are directionally oriented in such a way that their direction can be read based on their magnetic field.

Magnetic Density – The measurement of distance between individual magnetically aligned bits on a magnetic stripe; generally 210 bits per inch or 75 bits per inch, depending on the track. See Appendix B.

Magnetic Field – A physical property of magnetic materials, related to electrical currents; magnetic fields have a vector measurement of direction and magnitude, and can be observed with proper equipment.

Magnetic Stripe – A 0.330 inch strip of ferromagnetic material on a magnetic stripe card that is used to store data through magnetic alignment.

NFC – "Near Field Communication". A type of technology that can be read without physical contact; used in proximity cards rather than contact cards.

Parity Error Checking – A self-checking data feature that allows a system to detect if there was an error in reading binary information; functions by including an extra bit in each chunk of data that verifies either an even number of 1's (even parity) or an odd number of 1's (odd parity). See Appendix B.

PIN – "Personal Identification Number". A secret number known to the owner of a card, used to verify their identity during certain transactions.

Proprietary Information – Data stored on a magnetic stripe card that is known to the issuing body, but not necessarily to the user of the card; unique data used to verify identity and prevent data cracking.

Proximity Cards – A type of authentication card that can transmit data without physical contact.

RFID – "Radio Frequency Identification". A type of technology that can be read without physical contact; used in proximity cards rather than contact cards.

Security Administrator – The individual or group who designs and controls a security network designed for a specific purpose; in general the person who makes changes to a security network.

Security Network – The collection of security systems used in a particular environment or for a particular purpose.

Smart Cards – A newer type of authentication card technology that uses onboard memory or microcontrollers instead of a magnetic stripe; designed as either contact-cards or RFID cards.

Tracks – The areas on a magnetic stripe where information is stored; in general there are 3 tracks on one magnetic stripe, and each can be individually read from or written to.

Transferable Identity Verification Item – A type of security tool which is carried by the individual seeking authentication; used as a part of the identity-verification process of authentication and authorization.

Transient Magnetic Data – Card data that is meant to be changed every time the card is used; track 3 was designed to store transient data, but this practice has fallen out of use.

Usage Monitoring – The process of logging information about a magnetic stripe card's usage, and then using pattern recognition to prevent unauthorized authentication.

Verification Code – Supplemental data used to verify identity; in general either a number printed on the card and not on the magnetic stripe, or a PIN number known to the user.

Bibliography

[1] A Day in the Life of a Flux Reversal:
http://www.instructables.com/files/orig/F8F/O3U9/FJBYZ4T9/F8FO3U9FJBYZ4T9.txt

[2] IBM Magnetic Stripe Technology Origins:
http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/

[3] International Organization of Standardization:
http://www.iso.org/iso/home.html

[4] Magnetic Track Formats:
http://www.gae.ucm.es/~padilla/extrawork/tracks.html

[5] MSR606 Programmers Manual:
https://docs.google.com/file/d/0B9M7JgYQ-UQddEJzekdKdnpNejA/edit

[6] Financial Card Data:
http://blog.opensecurityresearch.com/2012/02/deconstructing-credit-cards-data.html?m=1

[7] Physical Security Manual & Checklist:
http://www.crimewise.com/airport/manual.pdf

[8] Onity Hotel Key Security Breach:
http://demoseen.com/bhpaper.html

[9] Smart Cards:
http://www.smartcardbasics.com/smart-card-types.html