Dumps Carding Tutorial

Introduction:

So youre interested in trying out instore carding? Instore carding is one of the fastest ways to get money. But you will need to keep your head on straight for this. As you should with every operation you go out to do. This tutorial will tell you the ins and outs of instore carding. Feel free to distrobute this as much as you want.

For the beginners:

Youre obviously reading this because you either A. Want to learn how to instore card or B. Want to see if you can find anything you are not aware of. For people who chose A. You should have atleast some prior knowledge of credit cards before you try instoring. If you do not that is ok too, just keep reading the tutorial and by the end of it you should be fine. The most important thing about instore carding is how you *Take the part* of the identity youre *Playinig* as. If youre going into a store looking to come out with $3-5k worth of electronics dressed in your normal apparel and being nervous, think again. You need to dress up and act like a person who would look like they could buy these items any day of the week. The first time youre going to be nervous ofcourse, its natural to be nervous the first few times. But with time and past experiences to look back on, it just gets easier as you go on.

Dressing the part:

This should come natural to most people out there. To buy something expensive you need to make it look like you can buy these items along with acting like you can (below). For your first operation i suggest should include you going into any of the clothing stores listed below and buy a decent amount of quality clothes. I cannot stress enough how quality plays a part in dressing up. Buying a sweater in walmart and a sweater in banana republic could determine the difference between getting out with your goods or running out of the store. Along with clothing you might want to buy some jewelry or a very high priced watch. If a cashier suspects something is up, seeing some classy jewelry or a watch could also help reduce the suspicion.

Clothing stores are usually never uptight with purchases of clothing so that is why I suggest going there first to get some quality clothes. You can be dressed as you want in there and it wont matter. When you buy the new clothes, put them on in a restroom and then continue your activities on a higher priced basis.

Acting the part:

This area will come hard for some but easier for others. Prepare yourself before you go in with things you might say. If youre going into a store to
buy smaller items ($800 and below) , this usually not hard to accomplish. But for larger items you

should act as if you can afford these items at any time of day. Acting stuck up in a sense can accomplish this. Other than that, dressing the part is the other area that helps you present yourself as a person of wealth.

Beginning:

Before you go out there and start instoring you will need the following items.

Card reader/writer - Youre going to have to (in most cases) need a card reader/writer to write new dumps on your cards. Especially if you want to re encode your cards and go out. The only case where you would not need this is if you were buying plastic from a vendor who offers to encode the dumps for you. For a reader/writer I highly recommend the MSR-206. It is the most popular encoder out there. You can buy them from

Price: $200 $640

Computer/Laptop (Preferred) - To be able to encode your dumps (later on) you will first need a computer to hook your card encoder up to. Using a desktop is fine but if you come into any problems with your dumps which is going to happen, you will have no way to re encode your plastic. You will have to drive home and re encode there. But if you have a laptop, you can bring your MSR with you and just hook it up and re encode while youre in your car. Doing this will save you gas, and time.

Price: $600 to $2400

Power Inverter - This is a very handy tool that youre going to need for this and you will probably find yourself using for all other types of things.

The MSR requires a power source so buy or card one of these. If your laptop battery gets low aswell which will sometimes happen just hook it up aswell. I found a very good one at BestBuy for $80. It covers up to 800 watts (400 watts each plug).
Price: $80

Plastic - I have seen all sorts of ways to obtain plastic. From stealing others and using those to buying them from a vendor. You DO NOT want to steal anyones credit cards and start using those. And you do not want to re encode your own credit cards. Im sure it makes sense to do so but over time if you start using your own credit card, the credit card companys are going to see the name being used and will surely contact you about these occurances. The best bet is to buy plastic from a vendor. Think about this too. When buying plastic, get atleast 2 cards with the same name as your novelty. It will save money on new novelties and give you a higher chance of walking out with your merchandise.

Dumps - The most important item of this whole operation. What would you do without dumps? Nothing thats what. I highly recommend snifferhack or linx101 for dumps. They supply the best quality on dumps. I have over 7-12 different dump vendor friends and I still stay strong with these 2. Now depending on what youre planning on getting out for your first op will determine on how much you will need to spend on dumps. I would not worry about spending for now. As soon as your op is over you will see that you have well made your money back from this.

Wallet - Some people may think that putting the plastic and novelty in your own wallet is not a bad idea. But the truth is that it is probably one of the biggest problems that could arise if anything was to happen. Keeping your false information and your real information seperate is a necessity. If you have any sort of personal contact information on you when carding I would suggest dropping it off in your car.

Optional Items -

Fake ID - HIGHLY RECOMMENDED but is not always needed. Most of the time for large purchases cashiers will ask for an identification that matches the plastic. There are numerous vendors out there who provide a novelty service that will fit your needs. Getting a state that is semi close to you is ideal in this situation.

Anonymous Phone - This is optional to have, I have used Chrome's dumps the most and he checks the dumps before sending so that all are valid. His dumps work 8/10 times on average. So if one card does not work I simply hand them another card with an excuse as to why that card was not working. When using a phone merchant there are two ways of authorizing a card. Some people think that charging a $1 or $1.50 on the card will not kill the card as many businesses use a $1 or $1.50 charge as a pre-authorization to check and see if the card is valid. Others prefer charging a random higher amount to make it look like a legit purchase. Either way, its up to you how would want to check it.

Serial to USB Converter - Smaller laptops may not come with a serial port to connect your encoder to. If this is the case you will need to buy one of these.

Price: $15-$25

Newskin Bandaid Liquid - You might be asking yourself "What would I do with this?". Well, if you really want to be protective you can put some newskin on your finger tips so no traces of fingerprints will appear on the plastic if any misfortune was to happen.

Planning:

Planning out what youre going to buy before you buy it would be a nice thing to do. It saves you time thinking of what you need or might need.

Also think about this. If youre main goal is to get a hefty sum of money, you should checkout ebay to see what sells for a high percentage. Usually gift cards to popular stores get high amounts back because they are just like cash. But just double check ebay.

If youre going to do an instore op for your own personal pleasure then you really dont need to make a list because you should already know what you want to get. Or you can look around in the store and choose what you want.

Taking care of business:

Before hand I always like going to the bathroom. It makes the carding situation a bit more easier if you get nervous. You do not want to get caught and be remembered as the kid who shit his pants. That is if you do get caught which odds are you wont if you follow these instructions.

Destination Safety:

Choosing a location to instore is not very hard. The internet has a vast amount of websites that have store locators. So find your subject mall or store and do a search to see whats around you. Here is a very important rule to follow by. Do not do anything where you live. Or in a more common way of putting it. Dont shit where you live. Find a store thats atleast a good half hour drive away from you and is atleast two cities over.

Some people choose to use fake license plates when entering your destination for carding just to add that extra level of security on in case a camera catches the car that drives away. This is ofcourse optional, but it doesnt hurt to put more safety on. Just dont speed away or anything that could get you pulled over.

Parking - When parking your car, make sure you park for out so no camera will catch your license plate. It will be worth the extra walk when youre walking out with your merchandise.

So now you have everything you need to get started. Youre prepared for the best and the worst situations to come.
The first time you go out you should expect some nervousness to come even before entering one of the stores listed below. The most important thing to do is to stay calm and act natural. The more suspicious you act, the more the cashier is going to suspect something is up. I do not recommend taking any drug or alcohol to calm yourself down. You need to look calm and natural while being alert to your atmosphere at the same time.

Anatomy of a dump:

B4111111111111111111^LASTNAME/FIRSTNAME^060910100 000000000000000000
4111111111111111111=06091010000000000000000000000

B - Identifies to the POS system that your card is a bank card

4111111111111111 - Credit Card Number

Lastname - Lastname of cardholder

/ - Seperater

Firstname - Firstname of cardholder

06 - Experation Year

09 - Experation Month

101 & Beyond - Bank data

Now some vendors will only sell the second track. So that leaves you with trying to figure out how to write track1. Most stores do not check track1 so it is not the most important thing. But to be safe I always include track1. Here is an example of what you will need to do. It is very easy.

4111111111111111=060910100000000000000

If you havent noticed, track2 in most cases is just like track1. To begin making track1, add a B that will indeicate its a Bank card.

B4111111111111111=060910100000000000000

Then, youre going to want to change the = to a
^lastname/firstname^ .

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000

And finally, youre going to add six zeros at the end of the dump.

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000000000

And thats your dump. Like I said its not hard to create track1 from only having track2. If you soley buy from BadB (soon ccoming back Smile) and linx,Script,Ryden or sniffer you will not have to do this.

Software to encode the dumps - I recommend TheJerms software. It is very self explanatory.

Types of dumps:

People ask me all the time about using generated dumps and if theyre good. I would not use generated dumps. Most of the time they will only work correctly with a certain Bin. And there is a 15% less success rate than using other types of dumps. You might as well use quality dumps in your locations you choose so people will not remember you instead of having errors come up and your face gets noticed more easily.

The best quality dump you will probably find are skimmed dumps. Skimmed dumps mean that the actual card was swiped onto a portable Mag Stripe reader. Therefore, using these you know you will have all of the correct information for track1 and track2.

Hacked dumps are usually taken from databases by you guessed it, hackers. The quality on these are the normal quality thats out there.

Dump types and limits:

I will only discuss so far visa, discover dump limits and a word on amex dumps as I have not encounted any use with mastercard dumps.

Visa Classic - These types of dumps are usually the cheapest to buy from a vendor. I have heard that on average you can get $500 on these types of dumps. But I have been pulled atleast $800 on them. Visa classics have a balance limit of $500 to $3,500. Although the most I have been able to get off of a single classic is $2,600 before an error occurs.

Visa Gold - One step above the classic, These limits start at $3,500 and can double as the cardholder gains good credit. With these you can make higher amounts of purchases.

Visa Platinum - Visa platinum dumps are for the larger purchases mainly. On a good day you can

pull off anywhere from $3,000 to $6,000 .

Visa Signature & Business - Signatues are said to have no limits. So for us that means these have the highest limits available. People have said to have gotten anywhere from $5,000 to $20,000 off of these types of dumps.

Discover - I have not used these that much in my past but from what I gathered you can get anywhere from $1,000 to $5,000 on these in one purchase. Using these dumps for multiple purchases will most likely kill the dump before you get past either of those limits. Almost all discover cards begin with a balance of $10,000.

Amex - I have not used these dumps. The reason to that is that you need the correct CVN to complete the transaction. It is not embossed, but printed onto the plastic. So you cannot re encode amex dumps. If the CVN is not correct when entered, you will automatically get a call for authorization.

How long dumps last:

This question no one can answer. You might be able to make a good prediction of how long they will last if you think of time and the dump type. For instance. If you have a classic dump, its 11:30 AM and you make a variety of small (Under $20) purchases. Odds are youre going to get that card to last a lot longer than a classic dump thats doing $300 purchases at 7:30 PM. Think of the cardholders work hours. They will usually be 9 AM to 5 PM. That is when their card is idle so to speak.

Choosing your cashier:

This is probably one of the more fun things to do while instoring. Usually 90% of the time, Minorities and Younger Girls make the best choice for cashing out. Minorities include, Blacks, Mexicans, and Asians if you were wonderings. The reason you want to choose these types for your cashiers are because they are usually the easiest to manipulate. In some cases you are going to have to use a normal person to cashout. But try not to make it a habit.

Interactions with the cashier:

In order to safely get your items out of the store successfully, you will need to know how to interact with the cashier. To in a sense manipulate them. When you bring your stuff up to the cashier act normal. If it is a large amount they might say something nice to you mentioning the amount of merchandise you are buying. Just play with it and make them feel good aswell. If you make the cashier not feel comfortable they will think something is up if any error happens. Which will sometimes if you are planning on doing a lot of instore.

Errors and Excuses:

As I was saying above, there are going to be errors now and then. Now most are very easy to talk your way out of. But in some cases youre going to need to know when you try and grab your novelty and card and just run. That will most likely not happen if youre only doing this a few times but for people who are planning to do this more often it is most likely going to happen atleast once. I have listed below a few common errors and how to handle them.

Optional Pre-Excuse - LWAI brought this excuse method to a lot of peoples attention and it is a very good idea in most cases. Making the cashier already think that the transaction will not go through so they are not surprised by the error, which makes handling the situation much easier. Saying something as easy as *I hope I have enough to cover this* or anything around those terms is good.

Declined - Once you spend and spend on a good dump there has to be an ending point. Usually with dumps that will not die this is the final step to completing it. Hopefully you will have another card on you to hand the cashier. If you don't thats fine too.

If you have another card - Oh, I thought that was going to happen. Here try my other card. If you do not have another card - I will be right back. I'm going to go get my check book / go to the ATM.

Call For Authorization - This one can be tricky if you do not have the right cashier. This is something you DO NOT want the cashier to do. A call for authorization is basically the store calling the bank or the stores authorization center in order to confirm that it is the actual cardholder making the purchase. If this happens just stay calm.

If you have another card - I don't have that much time, Ill call the bank later. Try my other card. If you do not have another card - I don't have that much time for this Ill call my bank and come back tomorrow.

If they persist on making the call, put your hand out as if they were going to give you your plastic back. Doing this tends to put some stress on the cashier as to whether or not give the card back to you. They usually will put the card back in your hands.

Do Not Honor - This will happen every now and then and is probably the easiest to overcome. The cashiers will sometimes just ask you if you have another card.

If you have another card - Hand them the card and say you'll call the bank about that one. If you do not have another card - Oh, I will call my bank about that tomorrow (then leave)

Those are the most common problems you are going to find. Of course there are more error codes.

There are about 50 of them. But by the time you manage to talk yourself out of these you will have enough experience to talk yourself out of the rest.

Selling your items:

There are a vast amount of ways for you to liquidate your items. The best way to do so is on ebay. I am not going to go into a large description because then this tutorial would change to how to sell your items or scam on ebay. You can either buy an account from a vendor or get a B&M bank account and create your own. I do not suggest using your own ebay account. A lot of people have in the past and even if a good amount havent been caught, you do not want to be that small percent that does.

Here is another area that can be done in a lot of ways. I will tell you to not put the money in your legit bank account. If you were thinking that, you should take a minute and think again. You could store your money on an electronic bank account service such as egold, or webmoney. Or if you want
more control over your money, you could keep it all in a well hidden safe. Using an electronic bank account instead has a higher security rate. As if anything was to happen to you involving LE, odds are they will not find your information for that account. Which means they would not have access to your
funds because they would not know it exists.

End Notes:

Thank you for taking your time to read this tutorial. I hope it was worth your time! I also hope that everyone who is inspired by this reply with any words or questions they would like to say. Good luck to all of you!

Merchant Codes:

Quote:00 Approved
01 Refer to Card Issuer
02 Refer to Card Issuer, special condition
03 Invalid Merchant
04 Pick up card
05 Do not honor
06 Error
07 Pick up card, special condition
08 Honor with identification
09 Request in progress
10 Approval for partial amount
11 Approved VIP
12 Invalid Transaction

13 Invalid Amount
14 Invalid card number
19 Re-enter transaction
21 No action taken
30 Format Error
41 Lost card Pick up
43 Stolen card Pick up
51 Not sufficient funds
52 No checking account
53 No savings account
54 Expired card
55 Pin incorrect
57 Transaction not allowed for cardholder
58 Transaction not allowed for merchant
61 Exceeds withdrawal amount limit
62 Restricted card
63 Security violation
65 Activity count limit exceeded
75 Pin tries exceeded
76 Unable to locate previous
77 Inconsistent with original
78 No account
80 Invalid transaction date
81 Cryptographic PIN error
84 Pre-authorization time to great
86 Cannot verify PIN
89 MAC error
91 Issuer unavailable
92 Invalid receiving institution id
93 Transaction violates law
94 Duplicate transaction
96 System malfunction

Part 2

What do I need for real carding?
This is a very good question you will need some cash. And the following will be helpful but not required at first. You should get these items at some point, but you don't need them right away. And I will tell you why in next section.

Computer-laptop is best, as you can carry it with you on your op?s if you desire. If you don't have a laptop you can use your home P.C. till you can afford to get one. Of course with home PC you cant take it with you on your ops

Encoder - If you look around most every has or talks about an MSR206 this seems to be the

preferred encoder, but you can also use an AMC722. The AMC722 is usually cheaper and does the same thing. Look on the net and you can find these for pretty decent prices. There is a internet company that will ship overnight and you can send payment by Western Union. The have a special for $550.00 you get MSR206 + Exeba Encoding Software + 50 loco or hico cards. Also XRAYSWIPE has pretty good deals on them also and is a reviewed vendor. You can use Exeba Comm software or TheJerm has a software program for the MSR206.

Laptop Bag - You can put your laptop and encoder in this also. Nice to have if you want to take your laptop and encoder on op?s.

Power Inverter - Needed to run your encoder and nice to have if out for long period of time and laptop is dying. You can get these just about anywhere even wallyworld.

Novelty Id - This should be at the top of your list as one of the first thing?s you should get. You will need this at some point you do not want to use your real info. I repeat do not even for 1 time use your real information. There are some good vendors that are quick also. Just look under the reviewed vendor section for more details.

Dumps - Get them from zeusk. You can get classic, gold, platinum, world, business, signature etc. If this is your first time you may want to get classic and start by shopping for low end items. IE anything under $200-$500. Now classics working not good and will go for 1 or 3 times that but the general rule of thumb is under $300 and you should be okay. Gold and Platinum for items above $500 but say to $1,000 and Business, Signature $1,000 and above. These are just suggestions and not hard rules.

Track 1 and 2 or just Track2 - you can get from zeusk. If you just have track2 only you can generate track 1 with PCKit-track1 generator. You will want to encode both tracks to your card. Making sure to change the name on the dump. Some stores only use track2 but it's best to stay safe and encode both.

Dump Example
Track1 B4100000000000000000^REGAN/RONALD^0409XXXXXXXXXXXXXXXXXX
Track2 4100000000000000000=04091XXXXXXXXXXXXXXXXXX

You of course change the name on track1 to your Novelty last name and first name.

Plastic cards to put dumps on: Okay again never use your own card to encode onto, just not the best idea. You can get cards from just about anywhere, some drugstores sell prepaid cc's, you can try that or get a Visa or MasterCard branded gift card. Most malls carry this type of GiftCard. Simon Cards have been used a lot in the past so I would suggest staying clear of those. The best way Buy from plastic vendor.

Wallet-You will need extra wallet to store you novelty items. You don?t want to use your own wallet and keep having to take you real cards and id out and replacing them with your novelty.

Anon Phone-Don't really need but if you have a phone merchant you can call from anon cell before going to use your card.

You don't need everything I have but they all are helpful.

Quick Start Up: Okay so you don?t have the time to wait to get all your tools or maybe your cash flow is not flowing. You may ponder how can I get up and going as quickly and cheaply as possible.

Answer: You can buy dumps from reviewed vendor of course and buy plastic from plastic vendor. Most plastic vendors will encode your cards for you. This may be the cheapest way to go. Say you buy 5 dumps for $50.00 = $250.00 and 5 plastic for $75.00 =$375.00 total for both $625.00. Add a drop to that $50.00 and for $675.00 you will be ready to go. Another advantage with going this route is you will have matching plastic. The plastic vendor will emboss your plastic with your novelty information. If you don?t have a lot of funds try taking a cash advance on your own card. You will be able to repay it rather quickly.

Okay I finally got everything, I'm Ready to go Right?

Answer: Okay hang on there Skippy, you may think you are ready but are you??

Get into The Correct Frame Of Mind: Remember you are the Cardholder this is your card and you will treat it as such. Repeat 50 times then say back words 25 times, lol, Just kidding but you are who you say you are. This is your card don?t be scared this is your card. Who?s Your Card? Also a good idea to be aware of what your novelty id says. Know the address etc, this will help you feel more at ease and will help if cashier ask off the wall question. Be prepared go over in your mind how different scenes might play out and have good sensible answers.

Remember the customer is always right, Never let them think you?re not legit even if they throw it in your face.

Pick Your Poison! (Where should I shop)
If you are a Newbie you should try stores with self swipe checkouts. Just beware some of the self swipes will verify your id. Also if you want to get your feet wet grocery stores with self swipe are real nice. They even have the ones that you ring up your own shit and pay without any cashier present.

Gas Stations- I would suggest staying away from gas stations. Most have cameras and why risk someone getting your car info for such a small purchase. Plus some dumps will die quickly when

using a Gas Station.

Using Cards with non-matching last 4- Simple shop at stores that do not check last 4 or use AVS or type in CW2 I?m not going to post which stores do and do not at this time. If you don?t know any off hand go there in person and use your legit card and watch what they do.

Cards with matching last 4- Shop anywhere that doesn?t have AVS or type in CW2 I will not list any stores you will have to do your own research.

What is AVS?

Address Verification System- verifies cardholders real addy, sometimes only uses zipcode.

Security- This is a very important topic, and here are some tips. First never park in front of store in which you are shopping. If someone gets suspicious of you they may write down your license plate or if they have cameras outside they may catch it on there cameras. Always park far enough away that the store cant see which car you got into. If possible park around a corner or have someone else drive and wait out of site for you. If you are using the buddy system You can get some 2 way radios or both keep cell phone on you and if shit hits the fan you can sprint away and have the car meet you somewhere nearby. Never run directly toward your car if shit hits the fan and you have the run, then security is probably running after you. See planning for more information on this. Also you may want to carry a small can of mace or pepper spray key chain size etc. This can be used to get your freedom from security but may lead to more charges if your caught.

Planning- Okay You are now just about ready to go.

1. What area will I be shopping at and what stores- Best to know in advance you can make driving directions to the area and from store to store. This is nice and will sped up the time your in one area. Helps you find the quickest way to and from area also. You don?t have to go this route you can go what I would call this free styling.

2. Once you spot your store find good parking spot away from camera out of view from store. Look around what will you do if shit goes wrong. A good rule of thumb is never run directly toward your car. You can park around the corner in next parking lot over. If shit hits fan you can exit store go in opposite direction and loop around behind the store to your car. Unless your 500 pounds and cant run in which if you try this method you may bet caught if you have to run.

3. Bring other Shirts with you. This is nice, you can change your shit when shopping at different stores this will help you keep much safer. And if your being chased you can take one off and have

the other one underneath.

4. Most of the time you wont have any problems and you may tire of parking so far away, you tell yourself I?ve done this 100 times and no problems. But never let your guard or security down. This is what keeps you safe plus it?s good to walk a bit for heath reasons.

5. Keep them guessing, some people wear hats and sunglasses. My advice don?t wear sunglasses inside it only makes you look shady. A easy way to change your appearance is to use real glasses. If you don?t wear glasses use Stage glasses these look like regular lenses but are clear with no prescription. If you already wear glasses try different frames or use contact lenses. Also you can change your facial hair, grow a mustache or a goatee or beard. Then shave it off after sometime and go bareback etc. These are ideas to change your appearence.

6. Dress the part, dress to fit in, you don?t want people to remember you.

7. Always shop a good distance from where you live. You don?t want them to catch you on camera and put a picture of you on the news for your family or friends to see. Also you don?t want to go back to the same stores using your legit information. It?s unlikely they will catch you but you can never be too safe.

Okay I?m ready

Okay you have your cards and dumps, you planned your op out and you have got your mind ready to go what?s next?

Shopping- Yeah let?s go, Remember this is your card. Be confident and act normal. Pick out your product proceed to cashier and check out. Choosing your cashier is vital and you will get rather good with this as you go from what I have heard. Usually younger females are the best. You want them to process you like everyone else. Make them feel they have no reason to ask for more information like id etc. If they ask for id show them , keep in your wallet and just hold it for the can see,
If they ask to see your card to compare signatures let them do it but keep you hand held out till they give it back. Start small and grow slowly , take time to learn the ropes and it will pay off for you big time.

Also if you card is declined it?s a good idea to carry a backup with you. You can tell them you might have overdrawn your account or limit and tell them you will try another card. If your 2nd card is declined or you don?t have one. Tell them you will go to bank or go get your checkbook etc. If for some reason you get a pick up card tell them you wife or girlfriend lost her card and reported her?s lost and you forgot. 99% of the time they will say okay. You can then try another card or tell them you will be back with checkbook.

Call for authorization- if this happens tell them you in a hurry and don?t have the time to deal

with that or tell them your card must be over the limit and you don?t want to purchase the item now. Act as a cardholder would act embarrassed. Whatever you do don?t go through with the call especially if they have your card in there hand.

What to stay away from- If you are new don?t try carding a laptop right away. Start small , I would suggest staying away from high fraud items IE laptops and electronics. Also stay away from high security stores i.e. BB and CC. And stay away from malls they have more security then you need to deal with in the beginning.

I will try and update this from time to time, feel free to give your input. Thanks and good luck!

Part 3

The following article explains practically how vulnerable banks are in the operation of ATM cards. ATM cards (Credit cards) usually has a magnetic stripe that contains the raw data called tracks for its operation.
The physical layout of the cards is standard. The LOGICAL makeup varies from institution to institution. There are some generally followed layouts, but not mandatory.
There are actually up to three tracks on a card.
Track 1 was designed for airline use. It contains your name and usually your account number. This is the track that is used when the ATM greets you by name. There are some glitches in how things are ordered so occasionally you do get "Greetings Bill Smith Dr." but such is life. This track is also used with the new airline auto check in (PSA, American, etc)
Track 3 is the "OFF-LINE" ATM track. It contains security information as your daily limit, limit left, last access, account number, and expiration date. (And usually anything I describe in track 2). The ATM itself could have the ability to rewrite this track to update information.
Track 2 is the main operational track for online use. The first thing on track to is the PRIMARY ACCOUNT NUMBER (PAN). This is pretty standard for all cards, though no guarantee.
Example of Track1
B4888603170607238^Head/Potato^0505101000000000120319180519100000 0
Example of Track2

4888603170607238=05051011203191805191
Usually only track1 and track2 are needed to exploit the ATM card.
Let us examine track1.

Take the Credit Card account number from Track 2 in this example it is:4888603170607238 and add the letter "B" in the front of the number like this B4888603170607238 then add the cardholder name YOU want to show on the card B4888603170607238^Head/Potato^(Last name first/First Name)next add the expiry date and service code (expiry date is YYMM in this case 0505,and in this case the 3 digit service code is 101 so add 0505101 ,

B4888603170607238^Head/Potato^0505101

No add 10 zero's after service code:

B4888603170607238^Head/Potato^05051010000000000

Next add the remaining numbers from Track2 (after the service code)

B4888603170607238^Head/Potato^05051010000000000012031918051 91

and then add six zero's (6) zero's

B4888603170607238^Head/Potato^0505101000000000012031918051910000000 this is your Track 1

Track 1:B4888603170607238^Head/Potato^0505101000000000012031918051910000000

REMEMEBER THIS IS ONLY FOR VISA AND MASTER CARD(16digits) , AMEX HAS 14 DIGITS, this doesn't work for Amex

FORMAT FOR TRACK2
CC NUMBER: YYMM (SERVICE CODE)(PVV)/(CVV)
Here is the Fleet's credit track2 dump:
4305500092327108=040110110000426
we see card number, an expiration date, 1011 - service code, 0000 is the place for pvn (but it is absent!), and at least 426 is the cvv (do not mix with cvv2)

Now let's take a look on MBNA's track2 dump:

4264294318344118=04021010000044500000
here we see the same - no pvn's and other verification information -just a cvv.

As clearly shown above it is possible to generate track1 from track2 using the method shown above. However track2 gen software automates the process.
The major process of getting the track2 info is through skimming. Fraudulent POS (Point of sale) merchants can use handheld devices called skimmers to read off and download the tracks data from your credit card if you are not careful. This is the main method of obtaining the original tracks from the credit card.
However this article will focus on the exploitation of ATM cards using credit card info such as Credit card number, cvv2, Exp date and PIN and then using algorithms commonly called ALGOS to generate the track2. These credit cards infos are normally obtained by spamming. There are a lot of reviewed [censored] who sells these infos in some carding forums.
Now it is interesting to note that there are a lot of talks about track2 generation possibility. How much is it real? However in my own candid opinion, it is very possible to generate track2. The simple truth is this.

Generation process of debit (and some credit) dumps from the credit card number, expiration date and cvv2 code becomes possible because of the banks' weak, "nonsaturated" structure and the banks failure to actually carry out proper validation of the track2 info. It might interest you to know that about 10% of banks are vulnerable. This vulnerability called pvv loophole have been fixed for the major banks But still sometimes the idiocy and negligence shown by employees of many American (and not only) banks quite often continues to surprise all: about 10% of issued cards still vulnerable, even for the moment.
During the last 2 years I have come to discover so many banks which are still vulnerable to this attack. This forms the basis of this article. Armed with the right tool, you can actually encode cards using cc number, cvv2, Exp date, PIN and the algos.
Now what is the nature of the algos you might ask? I will give you a sample.
518445**********=YYMM10100000000779
529107**********=YYMM10100000000CVV
These are track2 info. The RHS is the card number. YYMM is the exp date
(year/month) and the CVV is the card verification value. The first 6 digits of the card number is called the BIN . You only neeed to know if the BIN is casahble or vunerable to use the Algo.
Below is the screenshot of the Algo list I have compiled and tested to work 100% (About 800) .

Because some banks fail to actually validate the full track2 info, it is possible to use track2 generators softwares to attack the BINS. You simply enter the credit card number, cvv2, exp date and you get the generated track2. Remember this only works for weak BINS or cashable BINS. To test if the track2 you have generated is working before practically going to the ATM with the PIN to cash out, it is important you check the track2 using online checker. This will save cost for your embossed cards and it will be safer for you. I can offer you this service at a modest price of $3 for one track2 info. If you get 00 approval code and you have the right PIN , you will have about 97% success.

Part 4

n-Store Carding, the art of using conterfeit credit cards in order to obtain merchandise from stores. This article is for education only and to make those gain more knowledge

---
/Instore Carding Tips, Tricks,

"First things first:"

as trustfunded wrote, "this is your card", this is rule number one. you must convince yourself that this is your card. being paranoid, scared, or nervous is a perfect way to get busted and tip off a clerk or any employee of a store. you must appear like the ordinary customer, just like you were going to buy something legit. it is now 2006, the days of dumps working for weeks without a problem are not that common. banks are becoming more secure and pushing new methods of fraud tracing out all the time.

this will not go into how to encode dumps or talk about where to get them. refer to the forum to find this kind of stuff.

"security, the swipe,
when you go out to card instore it can go two ways. you can succeed or fail. if you succeed you will most likely be outside of the store without handcuffs on and some free shit in hand. if you fail, maybe you got a decline, call for auth, or maybe in the back of the police cruiser.

1. Keep your guard up:
personal security is the most important thing about pulling off one of these operations. be yourself, calm voice, do not ever say the word stole/steal/stolen/jacked/hacked in the store. you never know whos listening to you! park away from the store, walmart has cameras outside and can see your license plate. you may think you got away, but if the bank goes after you the FBI will damn sure see that camera feed.

2. Talk:
don't be scared to talk to the clerks about products, or anything! if you are very shy then maybe you ought to work on snapping out of it, being friendly with the clerk before the big swipe makes a huge difference. if pick out a older lady throw a stupid question out there such as "hows your day been" or "has it been busy? it has been so crowded everywhere during the holidays". maybe a young guy, "whats goin on man", "i went to a party last night and was smashed im so tired". sound stupid? well i'll tell you first hand it isn't, it WORKS.

3. Checkout:
when you first walk in, always scope out the register. see who is working, what kind of terminal it is (self swipe, etc), just so you do not run into something you don't want to mess with, whatever you do, DON'T stare over there because it might just make you look stupid or alert somebody because they believe you want to rob them or something.

a. Standing in line
standing in line just sucks, it really does. don't keep looking behind you. keep your head straight, don't laugh for no reason, and most importantly, do not look directly at a camera. talking is not necessary. a cell phone might be handy or maybe you can take a look at the product your getting.

b. the "swipe"
this is the most important part of instore carding, the swipe. this is where it goes down. if you have to hand the card over, go for it. as soon as the clerk swipes pull the hand out trick. put your hand over the register acting like you want the card back and most of the time they'll give it back. if not, then ask. you WANT, you NEED, you REQUIRE the card back. your prints are there so you better get it. if you self swipe, a good trick is to swipe it and put it away as fast as possible. not fast to where your practically going 400mph but you get the picture. this makes the clerk hesitate to ask you to see the card, compare signatures, whatever. all mind games here.

c. the "response"
you can get many results after the swipe, here we go.

- approved
you did it, sign that electronic screen or receipt and you are on your way. walk out and get the fuck out of there.

- declined
your cards fucked. either went too high or maybe it was a pick up. i never a clerk suspect a stolen card so i don't know what to suggest. throw them a 2nd card or if you don't have one, ask where an atm is and say you'll be back and just leave.

- call for authorization
tell that mother fucker you need the card back and all it means is that you went over your limit. if its self swipe tell them you have a thing and don't like giving your card to people because your bank said to keep it with you or some stupid excuse. calling for authorization on a card is bad news. some will just say declined, some will actually say "whats the name of the individual", and since you don't know, you're in a hot spot there. you can lie and say its your uncles and he told you to buy it maybe?

4. "where to go"
security is a big issue. i won't tell you all to stay away from malls because i shop there but never go back once you did it, although they have people walking around but most of the time they are looking for shop lifters. they have no reason to suspect you unless your banging out every store there and with a lot of people. any person with instore experience knows about the last 4 digits of the card. some POS terminals make the clerk type them in. if they don't match you are usually ok. tell them the bank is sending you a new card and you are sorry. you assumed you could still use it. radio shack, circuit city, best buy, hot topic, office depot(some), do last four. don't go there unless you spent money on matching plastic. good places to hit are stores inside of a plaza where there basically is no security besides LE patrolling the area which is usually fine. gas stations are easy but

they can kill the dumps in some cases. pay at the pump is a bad idea. i would only recommend it if you were shit broke and needed gas to do more carding. don't fucking gas up anywhere with cameras. next thing you know is you carded a brand new computer just to get busted for 20 dollars worth of gas.

Part 5- Pin Attacking

We present an attack on hardware security modules used by retail banks for the secure storage and verication of customer PINs in ATM (cash machine) infrastructures. By using adaptive decimalisation tables and guesses, the maximum amount of information is learnt about the true PIN upon each guess. It takes an average of 15 guesses to determine a four digit PIN using this technique, instead of the 5000 guesses intended. In a single 30 minute lunch-break, an attacker can thus discover approximately 7000 PINs rather than 24 with the brute force method. With a $300 withdrawal limit per card, the potential bounty is raised from $7200 to $2.1 million and a single motivated attacker could withdraw $30-50 thousand of this each day. This attack thus presents a serious threat to bank security.

1 Introduction

Automatic Teller Machines (ATMs) are used by millions of customers every day to make cash withdrawals from their accounts. However, the wide deployment and sometimes secluded locations of ATMs make them ideal tools for criminals to turn traceable electronic money into clean cash.

The customer PIN is the primary security measure against fraud; forgery of the magnetic stripe on cards is trivial in comparison to PIN acquisition. A street criminal can easily steal a cash card, but unless he observes the customer enter the PIN at an ATM, he can only have three guesses to match against a possible 10,000 PINs and would rarely strike it lucky. Even when successful, his theft still cannot exceed the daily withdrawal limit of around $300 . However, bank programmers have access to the computer systems tasked with the secure storage of PINs, which normally consist of a mainframe connected to a \Hardware Security Module" (HSM) which is tamper-resistant and has a restricted API such that it will only respond to with a YES/NO answer to a customer's guess.

A crude method of attack is for a corrupt bank programmer to write a program that tries all PINs for a particular account, and with average luck this would require about 5000 transactions to discover each PIN. A typical HSM can check maybe 60 trial PINs per second in addition to its normal load, thus a corrupt employee executing the program during a 30 minute lunch break could only make o with about 25 PINs.

However, HSMs implementing several common PIN generation methods have a
aw. The rst ATMs were IBM 3624s, introduced widely in the US in around 1980, and most PIN generation methods are based upon their approach. They calculate the customer's original PIN by encrypting the account number printed on the front of the customer's card with a secret DES key called a \PIN generation key". The resulting ciphertext is converted into hexadecimal, and the rst four digits taken. Each digit has a range of `0'-`F'. In order to convert this value into a PIN which can be typed on a decimal keypad, a \decimalisation table" is used, which is a many-to-one mapping between hexadecimal digits and

numeric digits. The left decimalisation table in Figure 1 is typical.

0123456789ABCDEF 0123456789ABCDEF
0123456789012345 0000000100000000

Fig. 1. Normal and attack decimalisation tables

This table is not considered a sensitive input by many HSMs, so an arbitrary table can be provided along with the account number and a trial PIN. But by manipulating the contents of the table it becomes possible to learn much more about the value of the PIN than simply excluding a single combination. For example, if the right hand table is used, a match with a trial pin of 0000 will conrm that the PIN does not contain the number 7, thus eliminating over 10% of the possible combinations. We rst present a simple scheme that can derive most PINs in around 24 guesses, and then an adaptive scheme which maximises the amount of information learned from each guess, and takes an average of 15 guesses. Finally, a third scheme is presented which demonstrates that the attack is still viable even when the attacker cannot control the guess against which the PIN is matched.

Section 2 of the paper sets the attack in the context of a retail banking environment, and explains why it may not be spotted by typical security measures. Section 3 describes PIN generation and verication methods, and section 4 describes the algorithms we have designed in detail. We present our results from genuine trials in section 5, discuss preventative measures in section 6, and draw our conclusions in section 7.

2 Banking Security

Banks have traditionally led the way in ghting fraud from both insiders and outsiders. They have developed protection methods against insider fraud including double-entry book-keeping, functional separation, and compulsory holiday periods for sta, and they recognise the need for regular security audits. These methods successfully reduce fraud to an acceptable level for banks, and in conjunction with an appropriate legal framework for liability, they can also protect customers against the consequences of fraud.

However, the increasing complexity of bank computer systems has not been accompanied by sucient development in understanding of fraud prevention methods. The introduction of HSMs to protect customer PINs was a step in the right direction, but even in 2002 these devices have not been universally adopted, and those that are used have been shown time and time again not to be impervious to attack [1, 2, 5]. Typical banking practice seeks only to reduce fraud to an acceptable level, but this translates poorly into security requirements; it is impossible to accurately assess the security exposure of a given aw,

which could be an isolated incident or the tip of a huge iceberg. This sort of risk management con

icts directly with modern security design practice where

robustness is crucial. There are useful analogues in the design of cryptographic algorithms. Designers who make \just-strong-enough" algorithms and trade robustness for speed or export approval play a dangerous game. The cracking of the GSM mobile phone cipher A5 is but one example [3].

And as \just-strong-enough" cryptographic algorithms continue to be used, the risk of fraud from brute force PIN guessing is still considered acceptable, as it should take at least 10 minutes to guess a single PIN at the maximum transaction rate of typical modules deployed in the 80s. Customers are expected to notice the phantom withdrawals and report them before the attacker could capture enough PINs to generate a signicant liability for the banks. Even with

the latest HSMs that support a transaction rate ten times higher, the sums of money an attacker could steal are small from the perspective of a bank.

But now that the PIN decimalisation table has been identied as an security relevant data item, and the attacks described in this paper show how to exploit uncontrolled access to it, brute force guessing is over two orders of magnitude faster. Enough PINs to unlock access to over $2 million can be stolen in one lunch break!

A more sinister threat is the perpetration of a smaller theft, where the necessary transactions are well camou
aged within the banks audit trails. PIN ver-
ications are not necessarily centrally audited at all, and if we assume that they are, the 15 or so transactions required will be hard for an auditor to spot amongst a stream of millions. Intrusion detection systems do not fare much better { suppose a bank has an extremely strict audit system that tracks the number of failed guesses for each account, raising an alarm if there are three failures in a row. The attacker can discover a PIN without raising the alarm by inserting the attack transactions just before genuine transactions from the customer which will reset the count. No matter what the policies of the intrusion detection system it is impossible to keep them secret, thus a competent programmer could evade them. The very reason that HSMs were introduced into banks was that mainframe operating systems only satisfactorily protected data integrity, and could not be trusted to keep data condential from programmers.

So as the economics of security
aws like these develops into a mature eld,
it seems that banks need to update their risk management strategies to take account of the volatile nature of the security industry. They also have a responsibility to their customers to reassess liability for fraud in individual cases, as developments in computer security continually reshape the landscape over which legal disputes between bank and customer are fought.

3 PIN Generation & Verication Techniques

There are a number of techniques for PIN generation and verication, each proprietary to a particular consortium of banks who commissioned a PIN processing system from a dierent manufacturer. The IBM CCA supports a representative sample, shown in Figure 2. We IBM 3624-Oset method in more detail as it is typical of decimalisation table use.

Method Uses Dectables
IBM 3624 yes
IBM 3624-Oset yes
Netherlands PIN-1 yes
IBM German Bank Pool Institution yes
VISA PIN-Validation Value
Interbank PIN

Fig. 2. Common PIN calculation methods

3.1 The IBM 3624-Oset PIN Derivation Method

The IBM 3624-Oset method was developed to support the rst generation of ATMs and has thus been widely adopted and mimicked. The method was designed so that oine ATMs would be able to verify customer PINs without needing the processing power and storage to manipulate an entire database of customer account records. Instead, a scheme was developed where the customer's PIN could be calculated from their account number by encryption with a secret key. The account number was made available on the magnetic stripe of the card, so the ATM only needed to securely store a single cryptographic key. An example

PIN calculation is shown in Figure 4.
The account number is represented using ASCII digits, and then interpreted as a hexadecimal input to the DES block cipher. After encryption with the secret \PIN generation" key, the output is converted to hexadecimal, and all but the rst four digits are discarded. However, these four digits might contain the hexadecimal digits `A'-`F', which are not available on a standard numeric keypad and would be confusing to customers, so they are mapped back to decimal digits using a \decimalisation table" (Figure 3).
0123456789ABCDEF
0123456789012345
Fig. 3. A typical decimalisation table
Account Number 4556 2385 7753 2239
Encrypted Accno 3F7C 2201 00CA 8AB3
Shortened Enc Accno 3F7C
0123456789ABCDEF
0123456789012345
Decimalised PIN 3572
Public Offset 4344
Final PIN 7816
Fig. 4. IBM 3624-Oset PIN Generation Method
The example PIN of 3F7C thus becomes 3572. Finally, to permit the card-holders to change their PINs, an oset is added which is stored in the mainframe database along with the account number. When an ATM veries an entered PIN, it simply subtracts the oset from the card before checking the value against the decimalised result of the encryption.
3.2 Hardware Security Module APIs
Bank control centres and ATMs use Hardware Security Modules (HSMs), which are charged with protecting PIN derivation keys from corrupt employees and physical attackers. An HSM is a tamper-resistant coprocessor that runs soft-ware providing cryptographic and security related services. Its API is designed to protect the condentiality and integrity of data while still permitting access according to a congurable usage policy. Typical nancial APIs contain trans-actions to generate and verify PINs, translate guessed PINs between dierent encryption keys as they travel between banks, and support a whole host of key management functions.
The usage policy is typically set to allow anyone with access to the host computer to perform everyday commands such as PIN verication, but to ensure that sensitive functions such as loading new keys can only be performed with authorisation from multiple employees who are trusted not to collude.
IBM's \Common Cryptographic Architecture" [6] is a nancial API imple-mented by a range of IBM HSMs, including the 4758, and the CMOS Crypto-graphic Coprocessor (for PCs and mainframes respectively). An example of the code for a CCA PIN verication is shown in Figure 5.
The crucial inputs are the PAN_data, the decimalisation table and the encrypted_PIN_block. The rst two are supplied in the clear and are straight-forward for the attacker to manipulate, but obtaining an encrypted_PIN_block that represents a chosen trial PIN is rather harder.
Encrypted_PIN_Verify(
A_RETRES , A_ED , // return codes 0,0=yes 4,19=no
trial_pin_kek_in , pinver_key , // encryption keys for enc inputs
(UCHAR*)"3624 " "NONE " // PIN block format
" F" // PIN block pad digit

```
(UCHAR*)" " ,
trial_pin , // encrypted_PIN_block
I_LONG(2) ,
(UCHAR*)"IBM-PINO" "PADDIGIT" , // PIN verification method
I_LONG(4) , // # of PIN digits = 4
"0123456789012345" // decimalisation table
"123456789012 " // PAN_data (account number)
"0000 " // offset data
);
```

Fig. 5. Sample code for PIN verication in CCA

3.3 Obtaining chosen encrypted trial PINs

Some bank systems permit clear entry of trial PINs from the host software. For instance, this functionality may be required to input random PINs when generating PIN blocks for schemes that do not use decimalisation tables. The appropriate CCA command is Clear_PIN_Encrypt, which will prepare an encrypted PIN block from the chosen PIN. It should be noted that enabling this command carries other risks as well as permitting our attacks. If there is not randomised padding of PINs before they are encrypted, an attacker could make a table of known trial encrypted PINs, compare each arriving encrypted PIN against this list, and thus easily determine its value. If it is still necessary to enable clear PIN entry in the absence of randomised padding, some systems can enforce that the clear PINs are only encrypted under a key for transit to another bank { in which case the attacker cannot use these guesses as inputs to the local verication command.

So, under the assumption that clear PIN entry is not available to the attacker, his second option is to enter the required PIN guesses at a genuine ATM, and intercept the encrypted PIN block corresponding to each guess as it arrives at the bank. Our adaptive decimalisation table attack only requires ve dierent trial PINs { 0000 , 0001 ,0010 , 0100 , 1000. However the attacker might only be able to acquire encrypted PINs under a block format such as ISO-0, where the account number is embedded within the block. This would require him to manually input the ve trial PINs at an ATM for each account that could be attacked { a huge undertaking which totally defeats the strategy.

A third and more most robust course of action for the attacker is to make use of the PIN oset capability to convert a single known PIN into the required guesses. This known PIN might be discovered by brute force guessing, or simply opening an account at that bank.

Despite all these options for obtaining encrypted trial PINs it might be argued that the decimalisation table attack is not exploitable unless it can be performed without a single known trial PIN. To address these concerns, we created a third algorithm (described in the next section), which is of equivalent speed to the others, and does not require any known or chosen trial PINs.

4 Decimalisation Table Attacks

In this section, we describe three attacks. First, we present a 2-stage simple static scheme which needs only about 24 guesses on average. The shortcoming of this method is that it needs almost twice as many guesses in the worst case. We show how to overcome this diculty by employing an adaptive approach and reduce the number of necessary guesses to 22. Finally, we present an algorithm which uses PIN osets to deduce a PIN from a single correct encrypted guess, as is typically supplied by the customer from an ATM.

4.1 Initial Scheme

The initial scheme consists of two stages. The rst stage determines which digits

are present in the PIN. The second stage consists in trying all the possible pins composed of those digits.
Let Dorig be the original decimalisation table. For a given digit i, consider a binary decimalisation table Di with the following property. The table Di has 1 at position x if and only if Dorig has the digit i at that position. In other words, Di[x] =
(
1 if Dorig[x] = i;
0 otherwise:
For example, for a standard table Dorig = 0123 4567 8901 2345, the value of D3 is 0001 0000 0000 0100.
In the rst phase, for each digit i, we check the original PIN against the decimalisation table Di with a trial PIN of 0000. It is easy to see that the test fails exactly when the original PIN contains the digit i. Thus, using only at most 10 guesses, we have determined all the digits that constitute the original PIN.
In the second stage we try every possible combination of those digits. Their actual number depends on how many dierent digits the PIN contains. The table below gives the details.
Digits Possibilities
A AAAA(1)
AB ABBB(4), AABB(6), AAAB(4)
ABC AABC(12), ABBC(12), ABCC(12)
ABCD ABCD(24)
The table shows that the second stage needs at most 36 guesses (when the original PIN contains 3 dierent digits), which gives 46 guesses in total. The expected number of guesses is, however, as small as about 23:5.
D10(p) ?= 00
p = 11
yes
D01(p) ?= 10
no
p = 10
yes
D01(p) ?= 01
no
p = 01
yes
p = 00
no
Fig. 6. The search tree for the initial scheme. Dxy denotes the decimalisation table that maps 0 ! x and 1 ! y.
4.2 Adaptive Scheme
The process of cracking a PIN can be represented by a binary search tree. Each node v contains a guess, i.e., a decimalisation table Dv and a pin pv. We start at the root node and go down the tree along the path that is determined by the results of our guesses. Let porig be the original PIN. At each node, we check whether Dv(porig) = pv. Then, we move to the right child if yes and to the left child otherwise.
Each node v in the tree can be associated with a list Pv of original PINs such that p 2 Pv if and only if v is reached in the process described in the previous paragraph if we take p as the original PIN. In particular, the list associated with the root node contains all possible pins and the list of each leaf should contain

only one element: an original PIN porig.
Consider the initial scheme described in the previous section as an example. For simplicity assume that the original PIN consists of two binary digits and the decimalisation table is trivial and maps 0 ! 0 and 1 ! 1. Figure 6 depicts the search tree for these settings.
The main drawback of the initial scheme is that the number of required guesses depends strongly on the original PIN porig. For example, the method needs only 9 guesses for porig = 9999 (because after ascertaining that digit 0{8 do not occur in porig this is the only possibility), but there are cases where 46 guesses are required. As a result, the search tree is quite unbalanced and thus not optimal.
One method of producing a perfect search tree (i.e., the tree that requires the smallest possible numbers of guesses in the worst case) is to consider all possible search trees and choose the best one. This approach is, however, prohibitively inecient because of its exponential time complexity with respect to the number of possible PINs and decimalisation tables.
It turns out that not much is lost when we replace the exhaustive search with a simple heuristics. We will choose the values of Dv and pv for each node v in the following manner. Let Pv be the list associated with node v. Then, we look at all possible pairs of Dv and pv and pick the one for which the probability of Dv(p) = pv for p 2 Pv is as close to 1
2 as possible. This ensures that the left and
right subtrees are approximately of the same size so the whole tree should be quite balanced.
This scheme can be further improved using the following observation. Recall that the original PIN porig is a 4-digit hexadecimal number. However, we do not need to determine it exactly; all we need is to learn the value of p = Dorig(porig). For example, we do not need to be able to distinguish between 012D and ABC3 because for both of them p = 0123. It can be easily shown that we can build the search tree that is based on the value of p instead of porig provided that the tables Dv do not distinguish between 0 and A, 1 and B and so on. In general, we require each Dv to satisfy the following property: for any pair of hexadecimal digits x, y: Dorig[x] = Dorig[y] must imply Dv[x] = Dv[y]. This property is not dicult to satisfy and in reward we can reduce the number of possible PINs from 164 = 65 536 to 104 = 10 000. Figure 7 shows a sample run of the algorithm for the original PIN porig = 3491.
No Possible pins Decimalisation table Dv Trial pin pv Dv(porig) pv
?=
Dv(porig)
1 10000 1000 0010 0010 0000 0000 0000 yes
2 4096 0100 0000 0001 0000 0000 1000 no
3 1695 0111 1100 0001 1111 1111 1011 no
4 1326 0000 0001 0000 0000 0000 0000 yes
5 736 0000 0000 1000 0000 0000 0000 yes
6 302 0010 0000 0000 1000 0000 0000 yes
7 194 0001 0000 0000 0100 0000 0001 no
8 84 0000 1100 0000 0011 0000 0010 no
9 48 0000 1000 0000 0010 0000 0010 no
10 24 0100 0000 0001 0000 1000 1000 yes
11 6 0001 0000 0000 0100 0100 0001 no
12 4 0001 0000 0000 0100 0010 0001 no
13 2 0000 1000 0000 0010 0100 0010 no

Fig. 7. Sample output from adaptive test program

4.3 PIN Oset Adaptive Scheme

When the attacker does not know any encrypted trial PINs, and cannot encrypt his own guesses, he can still succeed by manipulating the oset parameter used to compensate for customer PIN change. Our nal scheme has the same two stages as the initial scheme, so our rst task is to determine the digits present in the PIN.

Assume that an encrypted PIN block containing the correct PIN for the account has been intercepted (the vast majority of arriving encrypted PIN blocks will satisfy this criterion), and for simplicity that the account holder has not changed his PIN and the correct oset is 0000. Using the following set of decimalisation tables, the attacker can determine which digits are present in the correct PIN.

Di[x] =

(

Dorig[x] + 1 if Dorig[x] = i;

Dorig[x] otherwise:

For example, for the table Dorig = 0123 4567 8901 2345, the value of D3 is 0124 4567 8901 2445. He supplies the correct encrypted PIN block and the correct oset each time.

As with the initial scheme, the second phase determines the positions of the digits present in the PIN, and is again dependent upon the number of repeated digits in the original PIN. Consider the common case where all the PIN digits are dierent, for example 1583. We can try to determine the position of the single 8 digit by applying an oset to dierent digits and checking for a match.

Guess Oset	Guess Decimalisation Table	Customer Guess + Guess Oset	Customer Decimalised Original PIN	Verify Result
0001	0123 4567 9901 2345	1583	1584	1593 no
0010	0123 4567 9901 2345	1583	1593	1593 yes
0100	0123 4567 9901 2345	1583	1683	1593 no
1000	0123 4567 9901 2345	1583	2583	1593 no

Each dierent guessed oset maps the customer's correct guess to a new PIN which may or may not match the original PIN after it is decimalised using the modied table. This procedure is repeated until the position of all digits is known. Cases with all digits dierent will require at most 6 transactions to determine all the position data. Three dierent digits will need a maximum of 9 trials, two digits dierent up to 13 trials, and if all the digits are the same no trials are required as there are no permutations. When the parts of the scheme are assembled, 16.5 guesses are required on average to determine a given PIN.

5 Results

We rst tested the adaptive algorithm exhaustively on all possible PINs. The distribution in Figure 8 was obtained. The worst case has been reduced from 45 guesses to 24 guesses, and the average has fallen from 24 to 15 guesses. We then implemented the attacks on the IBM Common Cryptographic Architecture (version 2.41, for the IBM 4758), and successfully extracted PINs generated using the IBM 3624 method.We also checked the attacks against the API specications for the VISA Security Module (VSM) , and found them to be eective. The VSM is the forerunner of a whole range of hardware security modules for PIN processing, and we believe that the attacks will also be eective against many of its successors.

0

500

1000
1500
2000
2500
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Number of Attempts
Number of PINs
Fig. 8. Distribution of guesses required using adaptive algorithm

6 Prevention

It is easy to perform a check upon the validity of the decimalisation table. Several PIN verication methods that use decimalisation tables require that the table be 0123456789012345 for the algorithm to function correctly, and in these cases the API need only enforce this requirement to regain security. However, PIN verication methods that support proprietary decimalisation tables are harder to x.

A checking procedure that ensures a mapping of the input combinations to the maximum number of possible output combinations will protect against the rst two decimalisation table attacks, but not against the attack which exploits the PIN oset and uses only minor modications to the genuine decimalisation table. To regain full security, the decimalisation table input must be cryptographically protected so that only authorised tables can be used.

The only short-term alternative to the measures above is to use more advanced intrusion detection measures, and it seems that the long term message is clear: continuing to support decimalisation tables is not a robust approach to PIN verication. Unskewed randomly generated PINs stored encrypted in an online database such as are already used in some banks are signicantly more secure.

7 Conclusions

We are currently starting discussions with HSM manufacturers with regard to the practical implications of the attacks. It is very costly to modify the software which interacts with HSMs, and while update of the HSM software is cheaper, the system will still need testing, and the update may involve a costly re-initialisation phase. Straightforward validity checking for decimalisation tables should be easy to implement, but full protection that retains compatibility with existing mainframe software will be hard to achieve. It will depend upon the intrusion detection capabilities oered by each particular manufacturer. We hope to have a full understanding of the impact of these attacks and of the optimal preventative measures in the near future.

Although HSMs have existed for two decades, formal study of their security APIs is still in its infancy. Previous work by one of the authors [5, 4] has uncovered a whole host of diverse
aws in APIs, some at the protocol level, some
exploiting properties of the underlying crypto algorithms, and some exploiting poor design of procedural controls. The techniques behind the decimalisation table attacks do not just add another string to the bow of the attacker { they further conrm that designing security APIs is one of the toughest challenges facing the security community. It is hard to see how any one methodology for gaining assurance of correctness can provide worthwhile guarantees, given the diversity of attacks at the API level. More research is needed into methods for API analysis, but for the time being we may have to concede that writing correct API specications is as hard as writing correct code, and enter the traditional arms race between attack and defence that so many software products have to ght.

Acknowledgements
We would like to thank Richard Clayton and Ross Anderson for their helpful contributions and advice. Mike Bond was able to conduct the research thanks to the funding received from the UK Engineering and Physical Research Council (EPSRC) and Marconi plc. Piotr Zielinski was supported by a Cambridge Overseas Trust Scholarship combined with an ORS Award, as well as by a Thaddeus Mann Studentship from Trinity Hall College.
References
1. R. Anderson: Why Cryptosystems Fail Communications of the ACM, 37(11), pp32{40 (Nov 1994)
2. R. Anderson: The Correctness of Crypto Transaction Sets Proc. Cambridge Security Protocols Workshop 2000 LNCS 2133, Springer-Verlag, pp 125{127 (2000)
3. A. Biryukov, A. Shamir, D. Wagner Real Time Cryptanalysis of A5/1 on a PC Proceedings of Fast Software Encryption 2000
4. M. Bond, R. Anderson API-Level Attacks on Embedded Systems IEEE Computer Magazine, October 2001, pp 67{75
5. M. Bond: Attacks on Cryptoprocessor Transaction Sets Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES 2001), LNCS 2162, Springer-Verlag, pp 220{234 (2001)
6. IBM Inc.: IBM 4758 PCI Cryptographic Coprocessor CCA Basic Services Reference and Guide for the IBM 4758-001, Release 1.31. IBM, Armonk, N.Y. (1999) hxxp://www.ibm.com/security/cryptocards/bscsvc02.pdf

---
Part 6

Introduction:

So youre interested in trying out instore carding? Instore carding is one of the fastest ways to get money. But you will need to keep your head on
straight for this. As you should with every operation you go out to do. This tutorial will tell you the ins and outs of instore carding. Feel free to
distrobute this as much as you want.

For the beginners:

Youre obviously reading this because you either A. Want to learn how to instore card or B. Want to see if you can find anything you are not aware of.
For people who chose A. You should have atleast some prior knowledge of credit cards before you try instoring. If you do not that is ok too, just keep
reading the tutorial and by the end of it you should be fine. The most important thing about instore carding is how you *Take the part* of the identity
youre *Playinig* as. If youre going into a store looking to come out with $3-5k worth of electronics dressed in your normal apparel and being nervous,
think again. You need to dress up and act like a person who would look like they could buy these items any day of the week. The first time youre going
to be nervous ofcourse, its natural to be nervous the first few times. But with time and past experiences to look back on, it just gets easier as you go

on.

Dressing the part:

This should come natural to most people out there. To buy something expensive you need to make it look like you can buy these items along with acting
like you can (below). For your first operation i suggest should include you going into any of the clothing stores listed below and buy a decent amount
of quality clothes. I cannot stress enough how quality plays a part in dressing up. Buying a sweater in walmart and a sweater in banana republic could
determine the difference between getting out with your goods or running out of the store. Along with clothing you might want to buy some jewelry or a very
high priced watch. If a cashier suspects something is up, seeing some classy jewelry or a watch could also help reduce the suspicion.

Clothing stores are usually never uptight with purchases of clothing so that is why I suggest going there first to get some quality clothes. You can be
dressed as you want in there and it wont matter. When you buy the new clothes, put them on in a restroom and then continue your activities on a higher
priced basis.

Acting the part:

This area will come hard for some but easier for others. Prepare yourself before you go in with things you might say. If youre going into a store to
buy smaller items ($800 and below) , this usually not hard to accomplish. But for larger items you should act as if you can afford these items at any
time of day. Acting stuck up in a sense can accomplish this. Other than that, dressing the part is the other area that helps you present yourself as a
person of wealth.

Beginning:

Before you go out there and start instoring you will need the following items.

Card reader/writer - Youre going to have to (in most cases) need a card reader/writer to write new dumps on your cards. Especially if you want to re encode
your cards and go out. The only case where you would not need this is if you were buying plastic from a vendor who offers to encode the dumps for you. For
a reader/writer I highly recommend the MSR-206. It is the most popular encoder out there. You can buy them from
Price: $200 $640

Computer/Laptop (Preferred) - To be able to encode your dumps (later on) you will first need a computer to hook your card encoder up to. Using a desktop
is fine but if you come into any problems with your dumps which is going to happen, you will have no way to re encode your plastic. You will have to drive
home and re encode there. But if you have a laptop, you can bring your MSR with you and just hook it up and re encode while youre in your car. Doing this
will save you gas, and time. Price: $600 to $2400

Power Inverter - This is a very handy tool that youre going to need for this and you will probably find yourself using for all other types of things. The
MSR requires a power source so buy or card one of these. If your laptop battery gets low aswell which will sometimes happen just hook it up aswell. I
found a very good one at BestBuy for $80. It covers up to 800 watts (400 watts each plug). Price: $80

Plastic - I have seen all sorts of ways to obtain plastic. From stealing others and using those to buying them from a vendor. You DO NOT want to steal
anyones credit cards and start using those. And you do not want to re encode your own credit cards. Im sure it makes sense to do so but over time if you
start using your own credit card, the credit card companys are going to see the name being used and will surely contact you about these occurances. The
best bet is to buy plastic from a vendor. Think about this too. When buying plastic, get atleast 2 cards with the same name as your novelty. It will save
money on new novelties and give you a higher chance of walking out with your merchandise.

Dumps - The most important item of this whole operation. What would you do without dumps? Nothing thats what. Now depending on what youre
planning on getting out for your first op will determine on how much you will need to spend on dumps. I would not worry about spending for now. As soon
as your op is over you will see that you have well made your money back from this.

Wallet - Some people may think that putting the plastic and novelty in your own wallet is not a bad idea. But the truth is that it is probably one of the
biggest problems that could arise if anything was to happen. Keeping your false information and your real information seperate is a necessity. If you have
any sort of personal contact information on you when carding I would suggest dropping it off in your car.

Optional Items -

Fake ID - HIGHLY RECOMMENDED but is not always needed. Most of the time for large purchases cashiers will ask for an identification that matches the
plastic. There are numerous vendors out there who provide a novelty service that will fit your needs. Getting a state that is semi close to you is ideal
in this situation.

Anonymous Phone - This is optional to have, I have used dumps from seller that checks the dumps before sending so that all are valid. His dumps work 8/10 times on average. So if one card does not work I simply hand them another card with an excuse as to why that card was not working. If youre going through any other vendor you should buy a tracfone and find a phone merchant that will verify your dumps before you go
into a store. When using a phone merchant there are two ways of authorizing a card. Some people think that charging a $1 or $1.50 on the card will not
kill the card as many businesses use a $1 or $1.50 charge as a pre-authorization to check and see if the card is valid. Others prefer charging a random
higher amount to make it look like a legit purchase. Either way, its up to you how would want to check it.

Serial to USB Converter - Smaller laptops may not come with a serial port to connect your encoder to. If this is the case you will need to buy one of
these. Price: $15-$25

Newskin Bandaid Liquid - You might be asking yourself "What would I do with this?". Well, if you really want to be protective you can put some newskin
on your finger tips so no traces of fingerprints will appear on the plastic if any misfortune was to happen.

Planning:

Planning out what youre going to buy before you buy it would be a nice thing to do. It saves you time thinking of what you need or might need.

Also think about this. If youre main goal is to get a hefty sum of money, you should checkout ebay to see what sells for a high percentage. Usually gift
cards to popular stores get high amounts back because they are just like cash. But just double check ebay.

If youre going to do an instore op for your own personal pleasure then you really dont need to make a list because you should already know what you want
to get. Or you can look around in the store and choose what you want.

Taking care of business:

Before hand I always like going to the bathroom. It makes the carding situation a bit more easier if you get nervous. JediMasterC brought this on aswell.
You do not want to get caught and be remembered as the kid who shit his pants. That is if you do get caught which odds are you wont if you follow these
instructions.

Destination Safety:

Choosing a location to instore is not very hard. The internet has a vast amount of websites that have store locators. So find your subject mall or store
and do a search to see whats around you. Here is a very important rule to follow by. Do not do anything where you live. Or in a more common way of putting
it. Dont shit where you live. Find a store thats atleast a good half hour drive away from you and is atleast two cities over.

Some people choose to use fake license plates when entering your destination for carding just to add that extra level of security on in case a camera
catches the car that drives away. This is ofcourse optional, but it doesnt hurt to put more safety on. Just dont speed away or anything that could get you
pulled over.

Parking - When parking your car, make sure you park for out so no camera will catch your license plate. It will be worth the extra walk when youre walking
out with your merchandise.

Ready:

So now you have everything you need to get started. Youre prepared for the best and the worst situations to come.

The first time you go out you should expect some nervousness to come even before entering one of the stores listed below. The most important thing to do
is to stay calm and act natural. The more suspicious you act, the more the cashier is going to suspect something is up. I do not recommend taking any drug
or alcohol to calm yourself down. You need to look calm and natural while being alert to your atmosphere at the same time.

[color=blackImportant anatomy of a dump:

There is a more detailed version of this on CP. But for now, you will only need to know this information to start.

B4111111111111111111^LASTNAME/FIRSTNAME^060910100 000000000000000000
4111111111111111111=06091010000000000000000000000

B - Identifies to the POS system that your card is a bank card

4111111111111111 - Credit Card Number

Lastname - Lastname of cardholder

/ - Seperater

Firstname - Firstname of cardholder

06 - Experation Year

09 - Experation Month

101 & Beyond - Bank data

Now some vendors will only sell the second track. So that leaves you with trying to figure out how to write track1. Most stores do not check track1 so it
is not the most important thing. But to be safe I always include track1. Here is an example of what you will need to do. It is very easy.

4111111111111111=060910100000000000000

If you havent noticed, track2 in most cases is just like track1. To begin making track1, add a B that will indeicate its a Bank card.

B4111111111111111=060910100000000000000

Then, youre going to want to change the = to a
^lastname/firstname^ .

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000

And finally, youre going to add six zeros at the end of the dump.

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000000000

And thats your dump. Like I said its not hard to create track1 from only having track2.

Software to encode the dumps - I recommend TheJerms software. It is very self explanitory.[/color]

Types of dumps:

People ask me all the time about using generated dumps and if theyre good. I would not use generated dumps. Most of the time they will only work correctly
with a certain Bin. And there is a 15% less success rate than using other types of dumps. You might as well use quality dumps in your locations you choose
so people will not remember you instead of having errors come up and your face gets noticed more easily.

The best quality dump you will probably find are skimmed dumps. Skimmed dumps mean that the actual card was swiped onto a portable Mag Stripe reader.
Therefore, using these you know you will have all of the correct information for track1 and track2.

Hacked dumps are usually taken from databases by you guessed it, hackers. The quality on these are the normal quality thats out there.

Dump types and limits:

I will only discuss so far visa, discover dump limits and a word on amex dumps as I have not encounted any use with mastercard dumps.

Visa Classic - These types of dumps are usually the cheapest to buy from a vendor. I have heard that on average you can get $500 on these types of dumps.
But I have been pulled atleast $800 on them. Visa classics have a balance limit of $500 to $3,500. Although the most I have been able to get off of a
single classic is $2,600 before an error occurs.

Visa Gold - One step above the classic, These limits start at $3,500 and can double as the cardholder gains good credit. With these you can make higher
amounts of purchases.

Visa Platinum - Visa platinum dumps are for the larger purchases mainly. On a good day you can pull off anywhere from $3,000 to $6,000 .

Visa Signature & Business - Signatues are said to have no limits. So for us that means these have the highest limits available. People have said to have
gotten anywhere from $5,000 to $20,000 off of these types of dumps.

Discover - I have not used these that much in my past but from what I gathered you can get anywhere from $1,000 to $5,000 on these in one purchase. Using these dumps for multiple purchases will most likely kill the dump before you get past either of those limits. Almost all discover cards begin with a balance of $10,000.

Amex - I have not used these dumps. The reason to that is that you need the correct CVN to complete the transaction. It is not embossed, but printed onto the plastic. So you cannot re encode amex dumps. If the CVN is not correct when entered, you will automatically get a call for authorization.

How long dumps last:

This question no one can answer. You might be able to make a good prediction of how long they will last if you think of time and the dump type. For instance. If you have a classic dump, its 11:30 AM and you make a variety of small (Under $20) purchases. Odds are youre going to get that card to last a lot longer than a classic dump thats doing $300 purchases at 7:30 PM. Think of the cardholders work hours. They will usually be 9 AM to 5 PM. That is when their card is idle so to speak.

Advanced dump purchasing:

By now, if you have been reading about dumps. You might know that by purchasing dumps from banks that are closer to your area, that there is a higher success rate on most purchases. Only some vendors will offer to let you buy by a certain Bin (first six digits of the cc). The Bin determines what bank corresponds with the card. To find local Bins, go to http://www.hermesbank.net/interchange/ and search for a any bank that has a lot of locations in your area. You can also search for the state name and see what that comes up with.

Choosing your cashier:

This is probably one of the more fun things to do while instoring. Usually 90% of the time, Minorities and Younger Girls make the best choice for cashing out. Minorities include, Blacks, Mexicans, and Asians if you were wonderings. The reason you want to choose these types for your cashiers are because they are usually the easiest to manipulate. In some cases you are going to have to use a normal person to cashout. But try not to make it a habbit.

Interactions with the cashier:

In order to safely get your items out of the store successfully, you will need to know how to interact with the cashier. To in a sense manipulate them.

When you bring your stuff up to the cashier act normal. If it is a large amount they might say something nice to you mentioning the amount of merchandise
you are buying. Just play with it and make them feel good aswell. If you make the cashier not feel comfortable they will think something is up if any error
happens. Which will sometimes if you are planning on doing a lot of instore.

Errors and Excuses:

As I was saying above, there are going to be errors now and then. Now most are very easy to talk your way out of. But in some cases youre going to need
to know when you try and grab your novelty and card and just run. That will most likely not happen if youre only doing this a few times but for people
who are planning to do this more often it is most likely going to happen atleast once. I have listed below a few common errors and how to handle them.

Optional Pre-Excuse - JediMasterC brought this excuse method to a lot of peoples attention and it is a very good idea in most cases. Making the cashier
already think that the transaction will not go through so they are not surprised by the error, which makes handling the situation much easier. Saying
something as easy as *I hope I have enough to cover this* or anything around those terms is good.

Declined - Once you spend and spend on a good dump there has to be an ending point. Usually with dumps that will not die this is the final step to
completing it. Hopefully you will have another card on you to hand the cashier. If you don't thats fine too.

If you have another card - Oh, I thought that was going to happen. Here try my other card.
If you do not have another card - I will be right back. I'm going to go get my check book / go to the ATM.

Call For Authorization - This one can be tricky if you do not have the right cashier. This is something you DO NOT want the cashier to do. A call for
authorization is basically the store calling the bank or the stores authorization center in order to confirm that it is the actual cardholder making the
purchase. If this happens just stay calm.

If you have another card - I don't have that much time, Ill call the bank later. Try my other card.
If you do not have another card - I don't have that much time for this Ill call my bank and come back tomorrow.

If they persist on making the call, put your hand out as if they were going to give you your plastic back. Doing this tends to put some stress on the
cashier as to whether or not give the card back to you. They usually will put the card back in your hands.

Do Not Honor - This will happen every now and then and is probably the easiest to overcome. The cashiers will sometimes just ask you if you have another
card.

If you have another card - Hand them the card and say you'll call the bank about that one.
If you do not have another card - Oh, I will call my bank about that tomorrow (then leave)

Those are the most common problems you are going to find. Of course there are more error codes. There are about 50 of them. But by the time you manage
to talk yourself out of these you will have enough experience to talk yourself out of the rest.

Selling your items:

There are a vast amount of ways for you to liquidate your items. The best way to do so is on ebay. I am not going to go into a large description because
then this tutorial would change to how to sell your items or scam on ebay. You can either buy an account from a vendor or get a B&M bank account and
create your own. I do not suggest using your own ebay account. A lot of people have in the past and even if a good amount havent been caught, you do not
want to be that small percent that does.

Storing your money:

Here is another area that can be done in a lot of ways. I will tell you to not put the money in your legit bank account. If you were thinking that,
you should take a minute and think again. You could store your money on an electronic bank account service such as egold, or webmoney. Or if you want
more control over your money, you could keep it all in a well hidden safe. Using an electronic bank account instead has a higher security rate. As if
anything was to happen to you involving LE, odds are they will not find your information for that account. Which means they would not have access to your
funds because they would not know it exists.

End Notes:

Thank you for taking your time to read this tutorial. I hope it was worth your time! I also hope that everyone who is inspired by this reply with any
words or questions they would like to say. Good luck to all of you!

====

Stores:

Stores that do not type last 4:

7-11
Abercrombie & Fitch
Aeropostale
Almost every clothing store*
Albertsons
American Eagle
Amoura
Apple Store
Babbages
Barnes and Noble
Bath and Body Works
Body Shop
Bed Bath and Beyond
Bartel
Big 5
Blockbuster
Bose Factory Store/Showroom
Borders
Burlington Coat Factory
Cost Plus
Eddie Bauer
Every gas station (pay at pump)* Excluding Shell
Filenes
Foot Locker
Fred Meyer
FYE* (Some type last 4)
Gap
Garts Sports
Godiva Chocolates
Grocery Stores
Home Depot (self swipe)
JCPenny
Journeys* (Some type last 4)
Kauffman's
KB Toys
Kens Camera
Kmart (self swipe)
Lowe's (self swipe)
Linens and Things

Office Depot
Old Navy
Pier One Imports
Rite Aid
Safeway
SamGoody
Schucks
Sears
Spencer Gifts
Sports Authority
Staples* (Some type last 4, some dont)
Starbucks
Target (self swipe, sometimes check sig)
Timberland
Tower Records
Toy Works
Toys R Us
UPS Store
Victoria Secret
Walden Books
Walmart (self swipe but most check sig)
====

====

Restaurants:
Applebee's
Bertuccis
Chilis
Olive Garden
Pizza Hut
Papa Ginos
Unos
Wendys
*Almost all major restaraunts.
===

===

Stores that type last 4:

BestBuy
BurBerry
Circuit City (Uses AVS Aswell)
Cell Phone Services

CompUSA
Guitar Center
Hot Topic
Lindt Chocolates
Mens Warehouse
OfficeMax (Types In CVV on back of card)
SunGlasses Hut
Torrid
Tweeter

===

===
Merchant Codes:

00 Approved
01 Refer to Card Issuer
02 Refer to Card Issuer, special condition
03 Invalid Merchant
04 Pick up card
05 Do not honor
06 Error
07 Pick up card, special condition
08 Honor with identification
09 Request in progress
10 Approval for partial amount
11 Approved VIP
12 Invalid Transaction
13 Invalid Amount
14 Invalid card number
19 Re-enter transaction
21 No action taken
30 Format Error
41 Lost card Pick up
43 Stolen card Pick up
51 Not sufficient funds
52 No checking account
53 No savings account
54 Expired card
55 Pin incorrect
57 Transaction not allowed for cardholder
58 Transaction not allowed for merchant
61 Exceeds withdrawal amount limit
62 Restricted card
63 Security violation
65 Activity count limit exceeded
75 Pin tries exceeded

76 Unable to locate previous
77 Inconsistent with original
78 No account
80 Invalid transaction date
81 Cryptographic PIN error
84 Pre-authorization time to great
86 Cannot verify PIN
89 MAC error
91 Issuer unavailable
92 Invalid receiving institution id
93 Transaction violates law
94 Duplicate transaction
96 System malfunction

Part 7 Chip and Pin

Today we discuss a little about 201 dumps - a lot of peoples just running away once they seeing terrible number 201. Feel easy - things not so terrible.
First of all i would like to say that write 201 dumps on the chip it is not a fantastic, but is real things, and actually not so hard to do. But i want to discuss another thing - i would like to give you a hint how to use 201 dumps everywhere - even in such places where pos terminal requires chip...

Lets begin...
First thing we should have is a card with chip and magnetic stripe.Then we have to look pretty in the home for 12V AC adapter. Found. Good. Now all we have to do is to scratch a little chip metal contacts with + and - of the adapter. Seeing nice sparks - sign of good work ;-) After this little surgeon chip is not working anymore and this is extractly what we need. Now we have to encode 201 track to the regular magnetic stripe of the card and safely go to shop... Once the seller trying to insert the card with the chip he/she gets a nice error (additinally you can give him a reason that you washed your wallet with the card and chip is not working), and now most interesting part - once the terminal detects that chip is not fucntioning it switches back to magnetic stripe mode and allows you to swipe the card, all you have to do is to persuade the cashier to do it.

Part 8- Cracking Visa Pins

Have you ever wonder what would happen if you loose your credit or debit card and someone finds it. Would this person be able to withdraw cash from an ATM guessing, somehow, your PIN? Moreover, if you were who finds someone's card would you try to guess the PIN and take the chance to get some easy money? Of course the answer to both questions should be "no". This work does not deal with the second question, it is a matter of personal ethics. Herewith I try to answer the first question.

All the information used for this work is public and can be freely found in Internet. The rest is a matter of mathematics and programming, thus we can learn something and have some fun. I reveal no secrets. Furthermore, the aim (and final conclusion) of this work is to demonstrate that PIN algorithms are still strong enough to provide sufficient security. We all know technology is not the

weak point.

This work analyzes one of the most common PIN algorithms, VISA PVV, used by many ATM cards (credit and debit cards) and tries to find out how resistant is to PIN guessing attacks. By "guessing" I do not mean choosing a random PIN and trying it in an ATM. It is well known that generally we are given three consecutive trials to enter the right PIN, if we fail ATM keeps the card. As VISA PIN is four digit long it's easy to deduce that the chance for a random PIN guessing is 3/10000 = 0.0003, it seems low enough to be safe; it means you need to loose your card more than three thousand times (or loosing more than three thousand cards at the same time until there is a reasonable chance of loosing money.

What I really meant by "guessing" was breaking the PIN algorithm so that given any card you can immediately know the associated PIN. Therefore this document studies that possibility, analyzing the algorithm and proposing a method for the attack. Finally we give a tool which implements the attack and present results about the estimated chance to break the system. Note that as long as other banking security related algorithms (other PIN formats such as IBM PIN or card validation signatures such as CVV or CVC) are similar to VISA PIN, the same analysis can be done yielding nearly the same results and conclusions.

VISA PVV algorithm

One of the most common PIN algorithms is the VISA PIN Verification Value (PVV). The customer is given a PIN and a magnetic stripe card. Encoded in the magnetic stripe is a four digit number, called PVV. This number is a cryptographic signature of the PIN and other data related to the card. When a user enters his/her PIN the ATM reads the magnetic stripe, encrypts and sends all this information to a central computer. There a trial PVV is computed using the customer entered PIN and the card information with a cryptographic algorithm. The trial PVV is compared with the PVV stored in the card, if they match the central computer returns to the ATM authorization for the transaction. See in more detail.

The description of the PVV algorithm can be found in two documents linked in the previous page. In summary it consists in the encryption of a 8 byte (64 bit) string of data, called Transformed Security Parameter (TSP), with DES algorithm (DEA) in Electronic Code Book mode (ECB) using a secret 64 bit key. The PVV is derived from the output of the encryption process, which is a 8 byte string. The four digits of the PVV (from left to right) correspond to the first four decimal digits (from left to right) of the output from DES when considered as a 16 hexadecimal character (16 x 4 bit = 64 bit) string. If there are no four decimal digits among the 16 hexadecimal characters then the PVV is completed taken (from left to right) non decimal characters and decimalizing them by using the conversion A->0, B->1, C->2, D->3, E->4, F->5. Here is an example:

Output from DES: 0FAB9CDEFFE7DCBA

PVV: 0975

The strategy of avoiding decimalization by skipping characters until four decimal digits are found (which happens to be nearly all the times as we will see below) is very clever because it avoids an important bias in the distribution of digits which has been proven to be fatal for other systems, although the impact on this system would be much lower. See also a related problem not applying to

VISA PVV.

The TSP, seen as a 16 hexadecimal character (64 bit) string, is formed (from left to right) with the 11 rightmost digits of the PAN (card number) excluding the last digit (check digit), one digit from 1 to 6 which selects the secret encrypting key and finally the four digits of the PIN. Here is an example:

PAN: 1234 5678 9012 3445
Key selector: 1
PIN: 2468

TSP: 5678901234412468

Obviously the problem of breaking VISA PIN consists in finding the secret encrypting key for DES. The method for that is to do a brute force search of the key space. Note that this is not the only method, one could try to find a weakness in DEA, many tried, but this old standard is still in wide use (now been replaced by AES and RSA, though). This demonstrates it is robust enough so that brute force is the only viable method (there are some better attacks but not practical in our case, for a summary see LASEC memo and for the dirty details see Biham & Shamir 1990, Biham & Shamir 1991, Matsui 1993, Biham & Biryukov 1994 and Heys 2001).

The key selector digit was very likely introduced to cover the possibility of a key compromise. In that case they just have to issue new cards using another key selector. Older cards can be substituted with new ones or simply the ATM can transparently write a new PVV (corresponding to the new key and keeping the same PIN) next time the customer uses his/her card. For the shake of security all users should be asked to change their PINs, however it would be embarrassing for the bank to explain the reason, so very likely they would not make such request.

Preparing the attack
A brute force attack consists in encrypting a TSP with known PVV using all possible encrypting keys and compare each obtained PVV with the known PVV. When a match is found we have a candidate key. But how many keys we have to try? As we said above the key is 64 bit long, this would mean we have to try 2^64 keys. However this is not true. Actually only 56 bits are effective in DES keys because one bit (the least significant) out of each octet was historically reserved as a checksum for the others; in practice those 8 bits (one for each of the 8 octets) are ignored.

Therefore the DES key space consists of 2^56 keys. If we try all these keys will we find one and only one match, corresponding to the bank secret key? Certainly not. We will obtain many matching keys. This is because the PVV is only a small part (one fourth) of the DES output. Furthermore the PVV is degenerated because some of the digits (those between 0 and 5 after the last, seen from left to right, digit between 6 and 9) may come from a decimal digit or from a decimalized hexadecimal digit of the DES output. Thus many keys will produce a DES output which yields to the same matching PVV.

Then what can we do to find the real key among those other false positive keys? Simply we have to encrypt a second different TSP, also with known PVV, but using only the candidate keys which gave a positive matching with the first TSP-PVV pair. However there is no guarantee we won't get again many false positives along with the true key. If so, we will need a third TSP-PVV pair, repeat the process and so on.

Before we start our attack we have to know how many TSP-PVV pairs we will need. For that we have to calculate the probability for a random DES output to yield a matching PVV just by chance. There are several ways to calculate this number and here I will use a simple approach easy to understand but which requires some background in mathematics of probability.

A probability can always be seen as the ratio of favorable cases to possible cases. In our problem the number of possible cases is given by the permutation of 16 elements (the 0 to F hexadecimal digits) in a group of 16 of them (the 16 hexadecimal digits of the DES output). This is given by 16^16 ~ 1.8 * 10^19 which of course coincides with 2^64 (different numbers of 64 bits). This set of numbers can be separated into five categories:

1. Those with at least four decimal digits (0 to 9) among the 16 hexadecimal digits (0 to F) of the DES output.
2. Those with exactly only three decimal digits.
3. Those with exactly only two decimal digits.
4. Those with exactly only one decimal digit.
5. Those with no decimal digits (all between A and F).

Let's calculate how many numbers fall in each category. If we label the 16 hexadecimal digits of the DES output as X1 to X16 then we can label the first four decimal digits of any given number of the first category as Xi, Xj, Xk and Xl. The number of different combinations with this profile is given by the product 6 i-1 * 10 * 6j-i-1 * 10 * 6k-j-1 * 10 * 6 l-k-1 * 10 * 1616-l where the 6's come from the number of possibilities for an A to F digit, the 10's come from the possibilities for a 0 to 9 digit, and the 16 comes from the possibilities for a 0 to F digit. Now the total numbers in the first category is simply given by the summation of this product over i, j, k, l from 1 to 16 but with i < j < k < l. If you do some math work you will see this equals to the product of 104/6 with the summation over i from 4 to 16 of (i-1) * (i-2) * (i-3) * 6i-4 * 16 16-i ~ 1.8 * 1019.

Analogously the number of cases in the second category is given by the summation over i, j, k from 1 to 16 with i < j < k of the product 6i-1 * 10 * 6j-i-1 * 10 * 6k-j-1 * 10 * 616-k which you can work it out to be 16!/(3! * (16-13)!) * 103 * 6 13 = 16 * 15 * 14/(3 * 2) * 103 * 613 = 56 * 104 * 613 ~ 7.3 * 1015. Similarly for the third category we have the summation over i, j from 1 to 16 with i < j of 6 i-1 * 10 * 6j-i-1 * 10 * 616-j which equals to 16!/(2! * (16-14)!) * 102 * 614 = 2 * 103 * 615 ~ 9.4 * 1014. Again, for the fourth category we have the summation over i from 1 to 16 of 6i-1 * 10 * 616-i = 160 * 615 ~ 7.5 * 1013. And finally the amount of cases in the fifth category is given by the permutation of six elements (A to F digits) in a group of 16, that is, 616 ~ 2.8 * 1012.

I hope you followed the calculations up to this point, the hard part is done. Now as a proof that everything is right you can sum the number of cases in the 5 categories and see it equals the total number of possible cases we calculated before. Do the operations using 64 bit numbers or rounding

(for floats) or overflow (for integers) errors won't let you get the exact result.

Up to now we have calculated the number of possible cases in each of the five categories, but we are interested in obtaining the number of favorable cases instead. It is very easy to derive the latter from the former as this is just fixing the combination of the four decimal digits (or the required hexadecimal digits if there are no four decimal digits) of the PVV instead of letting them free. In practice this means turning the 10's in the formula above into 1's and the required amount of 6's into 1's if there are no four decimal digits. That is, we have to divide the first result by 104, the second one by 103 * 6, the third one by 102 * 62 , the fourth one by 10 * 63 and the fifth one by 64 . Then the number of favorable cases in the five categories are approximately 1.8 * 1015, 1.2 * 1012, 2.6 * 1011 , 3.5 * 1010, 2.2 * 109 respectively.

Now we are able to obtain what is the probability for a DES output to match a PVV by chance. We just have to add the five numbers of favorable cases and divide it by the total number of possible cases. Doing this we obtain that the probability is very approximately 0.0001 or one out of ten thousand. Is it strange this well rounded result? Not at all, just have a look at the numbers we calculated above. The first category dominates by several orders of magnitude the number of favorable and possible cases. This is rather intuitive as it seems clear that it is very unlikely not having four decimal digits (10 chances out of 16 per digit) among 16 hexadecimal digits. We saw previously that the relationship between the number of possible and favorable cases in the first category was a division by 10^4, that's where our result p = 0.0001 comes from.

Our aim for all these calculations was to find out how many TSP-PVV pairs we need to carry a successful brute force attack. Now we are able to calculate the expected number of false positives in a first search: it will be the number of trials times the probability for a single random false positive, i.e. t * p where t = 2^56, the size of the key space. This amounts to approximately 7.2 * 10^12, a rather big number. The expected number of false positives in the second search (restricted to the positive keys found in the first search) will be (t * p) * p, for a third search will be ((t * p) * p) * p and so on. Thus for n searches the expected number of false positives will be t * p^n.

We can obtain the number of searches required to expect just one false positive by expressing the equation t * p^n = 1 and solving for n. So n equals to the logarithm in base p of 1/t, which by properties of logarithms it yields n = log(1/t)/log(p) ~ 4.2. Since we cannot do a fractional search it is convenient to round up this number. Therefore what is the expected number of false positives if we perform five searches? It is t * p^5 ~ 0.0007 or approximately 1 out of 1400. Thus using five TSP-PVV pairs is safe to obtain the true secret key with no false positives.

The attack

Once we know we need five TSP-PVV pairs, how do we get them? Of course we need at least one card with known PIN, and due to the nature of the PVV algorithm, that's the only thing we need. With other PIN systems, such as IBM, we would need five cards, however this is not necessary with VISA PVV algorithm. We just have to read the magnetic stripe and then change the PIN four times but reading the card after each change.

It is necessary to read the magnetic stripe of the card to get the PVV and the encrypting key selector. You can buy a commercial magnetic stripe reader or make one yourself following the

instructions you can find in the previous page and links therein. Once you have a reader see this description of standard magnetic tracks to find out how to get the PVV from the data read. In that document the PVV field in tracks 1 and 2 is said to be five character long, but actually the true PVV consists of the last four digits. The first of the five digits is the key selector. I have only seen cards with a value of 1 in this digit, which is consistent with the standard and with the secret key never being compromised (and therefore they did not need to move to another key changing the selector).

I did a simple C program, getpvvkey.c, to perform the attack. It consists of a loop to try all possible keys to encrypt the first TSP, if the derived PVV matches the true PVV a new TSP is tried, and so on until there is a mismatch, in which case the key is discarded and a new one is tried, or the five derived PVVs match the corresponding true PVVs, in which case we can assume we got the bank secret key, however the loop goes on until it exhausts the key space. This is done to assure we find the true key because there is a chance (although very low) the first key found is a false positive.

It is expected the program would take a very long time to finish and to minimize the risks of a power cut, computer hang out, etc. it does checkpoints into the file getpvvkey.dat from time to time (the exact time depends on the speed of the computer, it's around one hour for the fastest computers now in use). For the same reason if a positive key is found it is written on the file getpvvkey.key. The program only displays one message at the beginning, the starting position taken from the checkpoint file if any, after that nothing more is displayed.

The DES algorithm is a key point in the program, it is therefore very important to optimize its speed. I tested several implementations: libdes, SSLeay, openssl, cryptlib, nss, libgcrypt, catacomb, libtomcrypt, cryptopp, ufc-crypt. The DES functions of the first four are based on the same code by Eric Young and is the one which performed best (includes optimized C and x86 assembler code). Thus I chose libdes which was the original implementation and condensed all relevant code in the files encrypt.c (C version) and x86encrypt.s (x86 assembler version). The code is slightly modified to achieve some enhancements in a brute force attack: the initial permutation is a fixed common steep in each TSP encryption and therefore can be made just one time at the beginning. Another improvement is that I wrote a completely new setkey function (I called it nextkey) which is optimum for a brute force loop.

To get the program working you just have to type in the corresponding place five TSPs and their PVVs and then compile it. I have tested it only in UNIX platforms, using the makefile Makegetpvvkey to compile (use the command "make -f Makegetpvvkey"). It may compile on other systems but you may need to fix some things. Be sure that the definition of the type long64 corresponds to a 64 bit integer. In principle there is no dependence on the endianness of the processor. I have successfully compiled and run it on Pentium-Linux, Alpha-Tru64, Mips-Irix and Sparc-Solaris. If you do not have and do not want to install Linux (you don't know what you are missing ;-) you still have the choice to run Linux on CD and use my program, see my page running Linux without installing it.

Once you have found the secret bank key if you want to find the PIN of an arbitrary card you just have to write a similar program (sorry I have not written it, I'm too lazy that would try all 10^4 PINs by generating the corresponding TSP, encrypting it with the (no longer) secret key, deriving the PVV and comparing it with the PVV in the magnetic stripe of the card. You will get one match for the true PIN. Only one match? Remember what we saw above, we have a chance of 0.0001 that

a random encryption matches the PVV. We are trying 10000 PINs (and therefore TSPs) thus we expect 10000 * 0.0001 = 1 false positive on average.

This is a very interesting result, it means that, on average, each card has two valid PINs: the customer PIN and the expected false positive. I call it "false" but note that as long as it generates the true PVV it is a PIN as valid as the customer's one. Furthermore, there is no way to know which is which, even for the ATM; only customer knows. Even if the false positive were not valid as PIN, you still have three trials at the ATM anyway, enough on average. Therefore the probability we calculated at the beginning of this document about random guessing of the PIN has to be corrected. Actually it is twice that value, i.e., it is 0.0006 or one out of more than 1600, still safely low.

Results

It is important to optimize the compilation of the program and to run it in the fastest possible processor due to the long expected run time. I found that the compiler optimization flag -O gets the better performance, thought some improvement is achieved adding the -fomit-frame-pointer flag on Pentium-Linux, the -spike flag on Alpha-Tru64, the -IPA flag on Mips-Irix and the -fast flag on Sparc-Solaris. Special flags (-DDES_PTR -DDES_RISC1 -DDES_RISC2 -DDES_UNROLL -DASM) for the DES code have generally benefits as well. All these flags have already been tested and I chose the best combination for each processor (see makefile) but you can try to fine tune other flags.

According to my tests the best performance is achieved with the AMD Athlon 1600 MHz processor, exceeding 3.4 million keys per second. Interestingly it gets better results than Intel Pentium IV 1800 MHz and 2000 MHz (see figures below, click on them to enlarge). I believe this is due to some I/O saturation, surely cache or memory access, that the AMD processor (which has half the cache of the Pentium) or the motherboard in which it is running, manages to avoid. In the first figure below you can see that the DES breaking speed of all processors has more or less a linear relationship with the processor speed, except for the two Intel Pentium I mentioned before. This is logical, it means that for a double processor speed you'll get double breaking speed, but watch out for saturation effects, in this case it is better the AMD Athlon 1600 MHz, which will be even cheaper than the Intel Pentium 1800 MHz or 2000 MHz.

In the second figure we can see in more detail what we would call intrinsic DES break power of the processor. I get this value simply dividing the break speed by the processor speed, that is, we get the number of DES keys tried per second and per MHz. This is a measure of the performance of the processor type independently of its speed. The results show that the best processor for this task is the AMD Athlon, then comes the Alpha and very close after it is the Intel Pentium (except for the higher speed ones which perform very poor due to the saturation effect). Next is the Mips processor and in the last place is the Sparc. Some Alpha and Mips processors are located at bottom of scale because they are early releases not including enhancements of late versions. Note that I included the performance of x86 processors for C and assembler code as there is a big difference. It seems that gcc is not a good generator of optimized machine code, but of course we don't know whether a manual optimization of assembler code for the other processors (Alpha, Mips, Sparc) would boost their results compared to the native C compilers (I did not use gcc for these other platforms) as it happens with the x86 processor.

The top mark I got running my program was approximately 3 423 922 keys/second using the AMD processor. So, how much time would need the AMD to break the VISA PIN? It would simply be the ratio between the size of the key space and the key trying rate, that is, 2^56 keys/3 423 922 keys/second ~ 2.1 * 10^10 seconds ~ 244 thousand days ~ 667 years. This is the time for the program to finish, but on average the true secret key will be found by half that time. Using commercial cryptographic cards (like the IBM PCI Cryptographic Coprocessor or the XL-Crypt Encryption Accelerator) does not help very much, they are, at most, 2 times faster than my top mark, i.e. it would take more than a hundred years to find the key, at best. Some more speed might be achieved (double, at most) by using a dedicated gigabit VPN box or similar hardware in a way surely not foreseen by the manufacturer ;-)

Even if you manage to get a hundred newest AMD or Pentium processors working in parallel it would still take more than 3 years to find the key (if they are provided with crypto-cards the time might be reduced to less than two years or to less than one year in case of a hundred gigabit VPN boxes). It is clear that only expensive dedicated hardware (affordable only by big institutions) or a massive Internet cooperative attack would success in a reasonable time (both things were already made). These are the good news. The bad news is that I have deliberately lied a little bit (you may already noticed it): VISA PVV algorithm allows for the use of triple DES (3-DES) encryption using a 128 bit (only 112 effective) encrypting key. If 3-DES is indeed in use by the PVV system you can still use the same attack but you would need four additional TSP-PVV pairs (no problem with that) and it would take more than 3 * 2^56 times more to find the double length key. Forget it.

PVV algorithm with triple DES consists in the encryption of the TSP with the left half of the encrypting key, then it decrypts the result with the right half of the key and encrypts the result again with the left half of the key. Note that if you use a symmetric 128 bit key, that is, the left half equals the right half, you get a single DES encryption with a single 64 bit key. In this case the algorithm degenerates into the one I explained above. That's why I did this work, because PVV system is old and maybe when it was implanted 3-DES was not viable (due to hardware limitations) or it seemed excessive (by that time) to the people responsible of the implementation, so that it might be possible some banks are using the PVV algorithm with single DES encryption.

Finally we can conclude that the VISA PVV algorithm as in its general form using 3-DES is rather secure. It may only be broken using specially designed hardware (implying an enormous inversion and thus not worth, see Wayner and Wiener) which would exceed the encryption rate of the newest processors by many orders of magnitude. However the apparently endless exponential growing of the computer capacities as well as that of the Internet community makes to think that PVV system might be in real danger within a few years. Of course those banks using PVV with single DES (if any) are already under true risk of an Internet cooperative attack. You might believe that is something very hard to coordinate, I mean convincing people, but think about trojan and virus programs and you will see it is not so difficult to carry on.

Part 9- UK Dumps

I am sure lot of people know about dumps, let look a bit deeper in to the dumps and how the are

authorised in UK. There are eight different main card types visa, master, debit visa, electron, solo and switch, etc. electron, solo and switch is similar to visa debit.

Solo
New customers get issued with solo; they are can upgrade to switch after three to six month. Solo will work almost everywhere in Europe as long as retailer PDQ accepts [cirrus, maestro]. I have no knowledge about outside Europe, dumps concise of 2 and 3 tracks apart from NatWest, which includes all three tracks. You can keep on using the dumps until all the money comes out.

Since most peoples wages goes in to the account direct, best time to use is any time after 28 each month, average wages being $1500 to $2000.

One good thing it lack the fraud protection, bad being only limited to UK and Europe, and its good only in the beginning of the month.

Switch
Is similar to solo only different being switch can guarantee cheques.

Electron
Is similar to solo, but you can use the electron anywhere, in the world its only good in end of the month.

Debit
I am sure that lot of people know about this, I think have to mention about Barclays debit, they use a new pattern spending software to authorise the cards, its good to use it in UK but you have one chance to use the dumps outside Europe, if it doesnt work once dont bother trying for less it want work.

Visa, Master
Generally dumps have high limit apart from few dumps, as far as to my knowledge capital one and Barclaycard offer lowest limit of $500, Barclays implement a pattern matching software which stops the unusual spending on the card, Barclays visa and master card will never work abroad,

Few things to remember about the dumps
To use the UK dumps, you don?t need to encode track 1 and 3, Track 2 is only authorised.
1111111111111111=11112011111111111111?
Have you noticed the 201 after the expiry date, which basically means that? When swiped on the PDQ, it will ask you to insert the embedded sim in to the reader.

Further more if its 101 then you will not asked for the sim, there are very few sim readable PDQ in UK. Don?t wary if you are going to use the dumps in other country you will not be asked to insert sim abroad, although I have heard from a friend that he was asked to insert the sim in one of the Middle Eastern country, I cant verify this.

Although one thing is certain you can use the dumps for only once if you purchase large amount. Debits and solos will defiantly work for more than once, If any one has any thing to add please do so.

Part 10

There are up to three tracks on magnetic cards used for financial transactions, known as tracks 1, 2, and 3. Track 3 is virtually unused by the major worldwide networks such as VISA, and often isn't even physically present on the card by virtue of a narrower magnetic stripe. Point-of-sale card readers almost always read track 1, or track 2, and sometimes both, in case one track is unreadable. The minimum cardholder account information needed to complete a transaction is present on both tracks. Track 1 has a higher bit density (210 bits per inch vs. 75), is the only track that may contain alphabetic text, and hence is the only track that contains the cardholder's name.
Track 1 is written with code known as DEC SIXBIT plus odd parity. The information on track 1 on financial cards is contained in several formats: A, which is reserved for proprietary use of the card issuer, B, which is described below, C-M, which are reserved for use by ANSI Subcommittee X3B10 and N-Z, which are available for use by individual card issuers:
Track 1, Format B:
Start sentinel — one character (generally '%')
Format code="B" — one character (alpha only)
Primary account number (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.
Field Separator — one character (generally '^')
Name — two to 26 characters
Field Separator — one character (generally '^')
Expiration date — four characters in the form YYMM.
Service code — three characters
Discretionary data — may include Pin Verification Key Indicator (PVKI, 1 character), PIN Verification Value (PVV, 4 characters), Card Verification Value or Card Verification Code (CVV or CVC, 3 characters)
End sentinel — one character (generally '?')
Longitudinal redundancy check (LRC) — it is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.
Track 2: This format was developed by the banking industry (ABA). This track is written with a 5-bit scheme (4 data bits + 1 parity), which allows for sixteen possible characters, which are the numbers 0-9, plus the six characters : ; < = > ? . The selection of six punctuation symbols may seem odd, but in fact the sixteen codes simply map to the ASCII range 0x30 through 0x3f, which defines ten digit characters plus those six symbols. The data format is as follows:
Start sentinel — one character (generally ';')
Primary account number (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.
Separator — one char (generally '=')
Expiration date — four characters in the form YYMM.
Service code — three digits. The first digit specifies the interchange rules, the second specifies authorisation processing and the third specifies the range of services
Discretionary data — as in track one
End sentinel — one character (generally '?')

Longitudinal redundancy check (LRC) — it is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.
Service code values common in financial cards:
First digit
1: International interchange OK
2: International interchange, use IC (chip) where feasible
5: National interchange only except under bilateral agreement
6: National interchange only except under bilateral agreement, use IC (chip) where feasible
7: No interchange except under bilateral agreement (closed loop)
9: Test
Second digit
0: Normal
2: Contact issuer via online means
4: Contact issuer via online means except under bilateral agreement
Third digit
0: No restrictions, PIN required
1: No restrictions
2: Goods and services only (no cash)
3: ATM only, PIN required
4: Cash only
5: Goods and services only (no cash), PIN required
6: No restrictions, use PIN where feasible
7: Goods and services only (no cash), use PIN where feasible
All values not explicitly mentioned above are reserved for future use
Notes:
It is possible for these strips to be completely erased if brought close to high strength Neodymium magnets[citation needed]
Commercial encoders might use '~' for Start sentinel, ';' for separator.
Example Code: '~#;data?'

Part 12 (part 12 has pictures so its in a pdf that should be bundled with this)

Dumps Carding Tutorial [Part 12]

This tutorial is pretty on point for the most parts, some aspects of what he is saying are a little extreme and unnecessary, however that all really depends on how paranoid you are.

Common sense, and right timing is all you really need to make it happen.

-Cryp

========== ==

I believe it’s not a secret to anyone that with the country’s decline of the economic situation, in a

geometrical progression, the level of criminal activity increases. Also, I think everyone is familiar with the well-known fact: that for any grand action – the counteraction should be even greater ... Why did I bring this up? ... During such hard times we all try to survive any way we can. That is why even those who have left this business for something legal are now coming back to old routs. And with the increase of our think-a-likes, so to say, - there is also an increase in those who think differently. I'm talking about competitors - COPS. Everything is rather simple in this world ... The more we steal the more they are trying to catch us, spending enormous amounts of money to do so. Unfortunately they don't understand and never will understand that we are not stealing – we are surviving. Well, actually they don't give a f**k. In this case if we shall ever meet face to face it would be impossible to explain anything, therefore we are better off not meet at all.

The conclusion is very simple: our safety comes first.

In this article we have decided to share our experience gained through almost 7 years of work. Currently we have people in almost all government agencies/ structures; therefore we have information about planned changes in the government's safety systems even before it's applied.

So ... How to cash out Damp + PIN and sleep peacefully at night, what is there to fear? And the most importantly – how are they trying to find us?

I'm sure everyone has their own methods and approaches, so we will not state that we are smarter then anyone else. We will simply tell about our approaches and applied tactics then everyone will make their own conclusions. I will only say that observing our rules and approaches, through the past 3 years, not one of our fighters has been caught.

1. The fastest and most productive way. We use it only for large amounts of a material, but unfortunately for the majority this is out of reach as it requires big capital investment. Not everyone can use this method, but for the general picture we have decided to share it.

Group or one person working on motorcycles.

Amounts that we did in half a day using motorcycles was 10 times greater than what the same group can execute in 3 days using cars. The point is that we can drive up to the ATM without even getting off the bikes. Black bike, black helmet - there are thousands of those in the city. Of course the bikes are without license plates and exclude any unique features.

For example ... All of our bikes have a toggle-switch for turning off the back light. In case if anyone follows you at night, you can become invisible almost momentarily. To give you an idea of what we do during daytime - we use 2 groups on 3 bikes each. Only 2 bikes are cashing and the third one just rides around. In case of danger during the routes – if COPS want to pull over one of the 2 bikes, 3rd bike will speed up or do some sharp movements (as it seems to COPS). Of course COPS will focus all of their attention on the escaping bike leaving alone the other two (filled with money and cards). So far COPS had no luck catching the escaping bike) we use "turbo charged HAYABUSA" motorcycles, but even if they do catch up ... maximum they can give a speeding

ticket, because that driver has nothing on him. We always leave a car near to the place of work. It is very convenient – just stop by for a few minutes every so often to drop off the money and empty cards.

This method is very effective but only for large cities, besides not everyone can drive a motorcycle and I am not even talking about their price.

2. Using a PICK UP TRUCK. All charm of this method is that it enables to hide the license plates easily and the most importantly - legally. Trucks overflow US roads, as they are very common and easily accessible. They do not attract much attention and can be easily lost in sight. Alright ... Everyone knows that in the US driving a car without front license plates is not a huge offence and COPS usually do not pay attention to that. But we still have the back license plate!? We pull down the trunk door and drive the car with an open trunk ... In this case the license plate is only visible to other drivers but absolutely not visible to cameras located on buildings. This allows parking near the ATM and accelerates your work.

Plastic.

Never use plain/ white plastic. It is not safe for many reasons. Someone can notice it and understand what's going on. If cops will find it – they will know what it's used for right away. And most importantly ... if such card is retained by the ATM and in the evening when workers take it out – they will understand what it is, they can make a police report and give it for examination which would reveal your finger prints. Just go to any grocery store and pick up some GIFT CARDS for example VISA or MC. These cards don't draw attention of any passer-bys; if COPS will find them, they will see them for what they are – gift cards, and the most importantly ... When workers will take it out from the ATM (if the card was retained), at least 10 people will touch the card – holding it in their hands and trying to figure out what moron wanted to take out CASH from a GIFT CARDS. At least this card will not go straight into a plastic bag for examination.

NEVER WRITE ON THE CARD!!!! Lately COPS are instructed on different signs to pay attention to in case of credit card detection. And so believe me... they examine each card at least for good 5 minutes. And God forbid a PIN is written on it. Use labels or mark the cards and keep the PINs separately.

ATM!!!

There are about 10 different kinds. Study them before beginning your work. If you see a small mirror - 90% chance that there is a CAMERA behind it. You see the black plastic square built into the panel by the pin pad or located by the monitor - 100% it’s a camera. You can’t hide from it but you can easily cover it with a sticker or something else. Cameras do not record all the time ... They start only after you have inserted the card in the ATM. Also, they shoot 15 frames per second - not 24 ... meaning that at reproduction the image recorded by the camera will be time-lapsed. And even if your face has got into the shot – don’t worry. It is impossible to find someone by the picture. ATM camera in mainly used for: when the card holder calls to the bank claiming stolen money - bank does an investigation and looks at the recordings from the camera. In 50% of the cases stupid Americans take their money themselves and then declare that someone has stolen it. Then bank tells the Americans about the cameras in the ATMs, and that the cardholder took out the money himself; and if they continue doing this - they can end up in prison. Therefore no one will search for the face in the camera shot. However if your license plates will get in the shot - that’s a different story.

Storage of cards!!!

Never keep all of the cards in your pocket. Hide them all in the car and take with you only the ones you will be using. By the law US COPS can search you in the street or for any small traffic violation. However, they cannot search your car. In other words ... for example they stopped you and searched you, if they have not found anything in your pockets - they will ask you to search your car. You can safely say NO!!! If you don’t have any pending warrants and nothing in your pockets – they would need a warrant to search your car. And they cannot get a warrant without a valid reason!!! We had a case when we were searched and asked to search the car ... We refused! After which the obnoxious COP said: we will now request a search warrant from the police department and will search your car. We nodded our heads and politely asked to sit in the car. In 20 minutes the COP told us that he is dispatched to an urgent call, threw our documents in our car and left. Clearly, no one can give him a search warrant without a legitimate reason. Before starting your work – get very familiar with the local laws.

Try to keep all of the cards hidden and the less possible on hands. However, if you are getting pulled over by COPS and you have a small amount of cards on hands - the best way is to dump them into the car door. When the window is open, there is a crack between the glass and the metal. Dumping the cards there - they fall directly inside the door. To get them the door would need to be disassembled and no one (COPS) would do that without a reason.

Communication facility!!!

Never keep your personal cell phone with you, as it is constantly registers by the operator – tracking your movement. For communication use only new phones activated specially for work and do not call anywhere besides another phone with the same purpose. Another example … for example your mobile phone works only with one operator (as previously iPhone) and approaching the ATM you are holding it in hands. Believe me, those looking for you can request the phone operator for all phone numbers which were registered in this region at that time ... Certainly the list will be long, but on the next report which they will request on another location (where you cashed out another ATM) same phone number will be precisely visible - the phone number which was in both places during required time....

Work in different city/ state.

Always remember that any card will work better at home. I am not even talking about REGION BLOCKS which is a big deal. And so … If the card is from one state and you start cashing it in another – the protection on UNUSUAL ACTIVITY works instantly and the bank will most likely call the cardholder. If the card is cashed in the same state - it will work much longer. It is already proven by us. So if you have a large amount of material from one place – think about it, maybe it's worth going there.

Another very important detail. When the cardholder calls his bank claiming someone stole his money - bank automatically sees the cardholder as suspected #1. Because the bank doesn't understand how and who can know the PIN code, that is known only to the owner. Maybe the bank understands, but it is easier to politely refuse giving a refund to the card holder due to lack of the INFORMATION CONFIRMING INNOCENCE of the OWNER. Sounds ridiculous, but it so ... the cardholder has to convince the bank of his innocence. That's why ... If you cash the card in other state - it will be easier for owner to prove that it wasn't him. If the bank knows that the owner is not guilty – they will start searching for the one who is. Well and if you bombed a card in a place of its residence – it will be hard prove cardholder's innocence and accordingly nobody will search for you … and if they will – it won't be soon.

I think everyone knows how to find out where the card is from.

Overlook your surroundings.

We always take a couple of days to examine local surroundings before starting work. During these couple of days we map out good/ rich and bad areas. We plan routes in advance: observe what time and how many COPS patrolling the area, also looking at the arrangement of banks and stand-alone ATMs. We find out where the bars and night clubs are located … In the evening there are many people – that is what we need. If you work at night we do not recommend using ATMs located in non-crowded places. Always remember that a patrol car can show up anytime and if you the only alive person in their sight – you will catch their attention. I recommend going to STRIP CLUBS ... you can look at the girls and the ATMs are good there. The limit on withdrawal is higher

than in bank ATMs and anybody will pay attention if you take money from 4-5 cards. That is a normal phenomenon there.

Part 13
ATM Skimmer Cashing/Installing Safety

I was many time asked questions about how to be secure when working with skimmers. I will try to describe here the basic moments, which are important in the work, about which it is not necessary to forget, and I will also write some recommendations from my own experience.

And so, let us begin from the fact that I recommend, first of all, to conduct an observation of the target ATM, in which you want to place your skimmer. Observation must be carried out unnoticeably, for a period of several days. Do not use only your memory when observing. Anyway all exactly will not be memorized, so that it is necessary to make notations, but such that only it could understand them. But after the end of observation to lead them into the normal mode. Observer must be located in the field of straight visibility, it is dressed must be imperceptible. Observation can be carried out both directly visually and by means of the optical objects, type of binoculars or camera. Purpose of the observer: to mark how much in what period (on the hours) comes card holders to ATM, to mark the servicing time of ATM by personnel or by collectors, mark time and periodicity of patrolling this region and mark the time of arrival and withdrawal of guards and workers of the adjacent stores and mark time and presence of the random persons, who can prevent work. For example old ladies, the street dogs, the spontaneous assemblages of people and so forth to analyze everything are proceeding for the elongation 2-3 days and to determine the optimum from the point of view of safety time of the installation of equipment on the ATM.