Credit Card Networks 101 What they are, and how to secure them

by Robert Imhoff-Dousharm

About this document

While this serves as a simi-detailed account of said speech at Def-Con 11, it does leave holes in material to be presented. Some things are better spoken out, and better interpreted by mannerisms and body language, or even overhead projector diagrams. Further, as I do hope this is at high levels of information to assist in learning of credit card networks, it cannot be complete due to exploits, and resolutions, unknown to me. My knowledge of this technologies my increase by the time this paper is published, and at a "best effort" I will disclose such information, if lacking here in. For these reason, please do not attribute below information as full, when considering "propagating" elsewhere.

Please also note that I will refer to mostly hotels and resorts in the document. These vendors have the largest vulnerable target currently in the credit card market. They are also more likely to have these type of systems due to their sheer size. Other market segments do have this networks, if you would like to know more about them, please drop the author a line

Introduction

Credit card networks have grown into a viable and necessary asset in large transaction based businesses. Are these networks protected? Are there formal security measures to protect these packets from external, and internal threats? Most network administrators, controllers(CTO) and CIO's are not even aware of credit card's flow or existence on a network. Further some over protect their switched network, disabling these systems from working correctly. One needs to have knowledge of these networks, know the possible exploits, and how to secure them.

Part 1 What are credit card networks, and what is their base design + introduction to credit card flow to bank

Section 1 How Credit card data gets from point A to point B

So what is the flow of credit cards? Does your card get swiped, then magically the money is removed from your account? Well obviously not. Lets take a look into what is involved.

So in a nutshell, your flow looks like this (see visual slide attached). Your card gets swiped at a credit card terminal, lets say a Visa card.   Then the information off your magnetic stripe gets put into a buffer on the terminal, or is sent to a main processing terminal on or off site. Using either a dial-up modem or a lease line, your card information is transmitted to a front end processor'. A front end processor works as a "Clearing house" for all banks associated with your card type. The FEP will then generate a transaction ID to your card. The processor will contact your bank electronically through a private lease line. It will ask two basic questions Is this a valid account at your bank? Does this account have "X" funds available? If your bank replies yes to both questions, the FEP will ask the bank to "Hold" (this is a very important point) "X" funds, for a preset amount of time, the bank will do so, then provide a 6 digit approval code to be sent back to the merchant. Here the FEP updates your transaction status in their system and adds an authorization flag. This flag will either be "A" for authorized, "D" for decline, or "R" for voice referral. There are some other flags, but they are for error reporting, and will not be coved here. Now the FEP sends a response back to the terminal at the merchant, and reports transaction guidance to the clerk, e.g. have customer sign receipt, call voice referral center for further guidance, decline acceptance of card. This is considered the "Authorization cycle" of a card.

At then end of every night, an auditor or clerk, will 'close' the credit cards that were swiped through out the day. When the cards are 'closed' this triggers the "Settlement Cycle". During this stage the terminal will contact the FEP through the dial-up or leased line connection. It will then upload a batch of cards, beginning with a totals report, and ending with a totals report. This is because cards do not get sent with error checking enabled, for security reasons. When your card gets 'closed', the FEP pulls up your transaction record, then checks your authorization code in the terminal with the one they have on file, it then contacts your issuing bank, and asks that funds be moved. The bank then uses a back end processor to move funds to the merchants account, this is automated through the F.E.P.

There are lots of extra steps involved, and manipulation of transfers in between. Today will be going over the added steps between the card swipe and the FEP, our credit card networks.

Section 2 How standard credit card networks work

In many situations, a credit card network is needed. Some examples are casinos, hotels, resorts, and retail chains. When you have a standard casino setup that includes four restaurants, one box office, one front desk, three bars, and a gift shop, getting all the cards balanced at the end of the night can be an interesting feat. Not to mention the IT over head in keeping these 'Island' terminals up and running. To reduce the headache of this nightly job, many large merchants have consolidated the process of authorizing cards, enter credit card networks.

In our casino example we have ten merchants that require multiple POS (point of sale) devices, and the ability to authorize cards. This site has a front desk property management system, a food and beverage software package (2 restaurants, 3 bars) and a lightweight POS system for the box office and gift shop. In the front desk setup, they have five terminals that can check clients into the hotel, all networked with Ethernet to a main server that is used for client tracking, and data mining. It can send credit card authorization request to an authorization terminal over the network to a credit card authorization server, and have it patch into a credit card FEP front end. Any time the cards are swiped, they will follow this path across your internal network. Our sample network has a grand total of 22 registers across 3 different types of POS systems, and they are from two different vendors. They are connected to the CC Server using an API approach, all moving across ethernet to get there. This is a typical setup at many resort and casino's, especially here in town (Las Vegas, NV, USA).

With our sample network shown above, there are lots of area's for exploits, especially in the hospitality industry. So what are this risks? Where do they come from?

Part 2 The inherit risks from simple to complicated

Section 1 Social Engineering

a) Getting money using a credit card terminal

How can we use our charisma to get vendor information, and free money? With the above network style's in a very infant stage currently, there are lots of kinks to be worked out.

If you have the right tools, and TLA's, you can get what you need from a merchant. Call a hotel, say your with an issuing bank, and you need there voice merchant account of that site. You need this to verify that their client was actually at your hotel, and you think someone is using a card in a fraudulent way. Hell give them your credit card number if they want to look up the guest, they won't find it, but will give you the voice referral merchant ID. Step one is done!

Call their F.E.P. give them the merchant ID, let them know that there is a problem with your credit card terminal. Ask if they can help you re download the terminal. They will gladly help out. Using your own credit card machine, you follow there instructions, and get a fresh terminal. Wow! Now you have your very own money making machine! Give you and your friends credits (to a Swiss bank?). Buy an unsecured credit card from Walgreens and they will activate your own non-existents bank account! You money launders can figure out the rest from there.

b) Getting money directly from the merchant

Through my travels in the credit card industry, I have seen many - for lack of a better word - ignorant clerks and auditor. One good example was this 200 room hotel, with a jittery accounting auditor. She reported that a front desk clerk attempted to authorize a client card, and the bank responded with a decline. The clerk let the guest check in anyway, stating that they would need to get payment fixed on check out. This guests card account was closed, and they knew that it would not go through. When they left, with an outstanding bill, the hotel had to "zero" the balance without receiving money. So instead of voiding the card from their PMS system, they issued a credit to zero the system! That's right, they gave the declined card over $1000 USD!

So what can this tell us about social engineering at the merchant level? It's a lot easier to get money from a hotel, then to get cell phone source code from Nokia. You have photo shop and on-line banking right? Can your statement printout show 2 charges on your card suddenly? Sure it can. Faxing it to a hotel to get the second charge reversed to a credit, sure why not! Does it work, yes. This summer alone, I have spotted over 20 fraud clams based on this concept, because auditors were confused if they should issue a credit. 2 of which they sent a credit to their client, then called call me for assurance!

Section 2 Network and Internet based attacks

a) Attacking from inside the network

Using shared networks. Too often a hotel will boost "we have Internet access in every room, and Wi-Fi in the lobby!" and not realize that they are giving their customers access to the same shared media as their credit cards!

The latest crazy in resorts and hotels, large and small, is high speed Internet access. They love to boast that they have Wi-Fi access points in their lobby, and Internet hook-up's in every room. This is a great point of attack for anyone who would like to gain access to credit card numbers. Remember in the credit card network example, all of the point of sales systems connect to the main authorization engine using an API approach over ethernet. The company usually does not put firewalls in place to segregate cooperate traffic, and guest traffic. Thus a simple port sniffing program, similar to F.B.I.'s carnivore, can grab all the packets on their network. Once you have your target computers IP, based on collected packets, you can grab all the credit card packets from the PMS to the terminal all day long. While this will obviously give you access to all the card numbers, and expiration date, it also give you something more important, swipe data. With swipe data, you can use this to create your very own cards, based on information collected. This is assuming you have a card magnet machine, which is not cheap. But any pro can just walk in and have a field day. Even for the weekend hacker, just having CVV2 data, Names, zip codes, card numbers, expiration date, should do just fine as well.

b) Attacking from outside the network in

Now what if they don't provided Internet access to their clients, how could we get card data? Through their non-existent firewall. Picture this I get a call in from a site that just got setup. They report that their credit card terminal is not authorizing cards. So first I check to see if the software is running correctly. On the software, it reports that there is an Internet connection problem. I ask the client about his network, and how he connects to the Internet, it went something like this,

"Oh I have 3 computers connected to this LinkSYS firewall / router / switch. Yeah this thing is great, it connects all my computers to the Internet". I nearly shit a brick.
"So you have your credit card terminal going out to the Internet through this device, with no firewall to protect your network?" I inquire.
"No, no, it is a firewall router combo, see I do have a firewall protecting me!" He proclaims.
"Does it deny incoming packets on X port? You know the one that our software is running on?"
"Uh, well, I don't know what X port is, or what a "port" is, is this bad?"

Lets elaborate a possible situation. I'm a port scanning freak, doing the rundown of the neighbors on my net block, and I run across a response on "X" port from this guys so called "firewall". "Why what is this?". I quickly start monitoring packets, and find credit card data! Jackpot! Good for me, not good for $59 all in one router hotel. Get the point? So what are you waiting for start scanning!

Section 3 Reading ip packets from a PMS to a credit card terminal

When sending credit card packets across a "trusted" network, there usually is no encrypting of data. So when you grab these packets, they are usually clear text. So how do we understand what really in them?

Writing the code for an API interface can be pretty straight forward on the socket end, open a port and listen for incoming traffic, when received, examine data, and push to an authorization process. So how can we read the data coming in on said open port? Well this data can be sent three basic ways ASCII (clear text), binary, or as encrypted traffic (which would first be unwrapped, then sent to get authorized. Since this data is coming from a different (usually) vendors software, they usually same their programers the time, and only have ASCII sent across from their interface. This is of course, overly simplified, but will use this for our example.

Most packets that come across usually do not need to be read in a hex editor, just opening notepad, and sifting through the junk will be enough. With these packets, certain fields must be transmitted (card number, exp date, dollar amount, etc.). If it is coming across clear it will usually read

Client Name X
Card Number X
EXP Date X
Invoice X
Auth Type X
AVS X
CVV2 X
Primary Amount X
Secondary Amount X

This will have date and time marked with each line of information, and there are dozens of other fields that can be sent as well, such as corporate ID (for lower discount rates) and checksum information. The point here is, after staring at your captured data, it will only take about 5 min to figure out what is what from an ASCII data stream, as surprisingly, programers make transmission of this data very high level.

Section 4 The ex-employee

So you can't get the grasp of the check-in process, or you really don't know how to balance the books that well, so the company let you go. But, you didn't think this was fair, you tell all your friend that this hotel is a shady place, and the manager is a prick. What if one of those friends was 1337, and took interest in this...

So your jerk-off friend, who has a different job every other month tells you that his last one was bull shit. He goes on to say "That place is a dump, hell one time the manager change my password and didn't tell me". You push for him to tell you more. "Well, it's everyone's password, he did it on accident, because he though he was logged in with his account". Everyone's passwords? "Yeah, we all logged in with the same user and password, why?"

So you take that user name and password, and get out of him that they use "2000Blue front desk suite". You learn about this software, and pay a visit to the hotel. "Hi, I'm Joe from 2000Blue, I came to apply a patch to your software, Jake "the boss" Johnson should have called to tell you I was coming in..." Or. Stop on by when they have low volume at front desk, hop in and drop your key logger / spyware into the system, you have the password. Now you get emailed credit card numbers!

In summary, you all have big imagination with what you could do with default user name/passwords, have a field day!

Section 5 The main point

When you have a small medium or large business, it's always important to have good security. Most of these examples, and my credit card experience, is in the hospitality industry. For some odd reason, they never got the memo that security is a good thing. Most are focused on "Customer Satisfaction" "Tai Chi / Guest experience" and, for smaller hotels, easy money with a simple business plan. This leaves the hotel industry wide open for exploits when the upgrade their credit card authorization to internal networks tying into modems and the Internet. Even with the flood of computer professionals on the market, they look to the bottom line, and cannot justify "proactive" hiring, only seasonal "reactive". Further the credit card industry is very loose and dynamic right now. There are many unregulated area's, even for an industry as sensitive as it is. There has been no real push to make it fully secure, so this leaves us with a new target to lean in on.

What if I did work at a hotel, and I wanted to protect my card assets? What would be necessarily? Is it all that hard to secure my credit card networks?

Part 3 How this can be avoided

Section 1 Protecting against social engineering

There are many different ways to protect against this method, good and bad. When a client of mine went overboard, and thought he was being attacked by terrorist, calling his manager and demanding the police put a trace on his phone- This for me calling in to do a software patch update - things can obviously get out of hand. But it does not have to be that tight. If someone calls in to do work, call them back, listen for an automated service that give out the company name. Check that the number they provide is the same you have on file when you call them. Call the vendor back, but only with the support number you have.

When people want free money from you, sometimes training the whole staff will not get the message across, and it can coast too much, if it will only happen once to you. Delegate one or two people, maybe an auditor, who can handle charge back requests exclusively. Always, always, always call your bank to verify that money was or was not deposited into your account from said client, don't assume your system is right, or the client for that matter. This applies, even if they fax a statement in.

Section 2 Protecting your network

What merchants fail to understand is that they have a large amount of sensitive data going across their network, and they have no concept of "Plugging holes". Even in a half-hearted way. We are in the middle of a bad recession, now more then every merchants are using "If it's not broke..." analogy's to justify why they leave back doors open. They refuse to invest money into protected their most valuable assets, their clients. Even still, just investing in good security practices, and making even a modest investment in network security would close 99% of the hacks they are currently exposed to.

Using unique ID's is not just good practice, it is a regulation for anyone entering in, or accessing credit cards to a credit card network. Limiting access and rights also falls under this category. Make sure when someone gets fired, their accounts are deactivated. Have cooperate traffic separate from client "in room" traffic, and Wi-Fi hot spots in the lobby is also essential. Having a business class firewall is required for all merchants who propagate traffic across the Internet, secured or not. When big credit card vendors (Visa, Master Card, etc) really start their audit of merchants, fines can and will be accrual, and acceptance rights will be revoked. This of corse, is pretty obvious to you, but not to the non-existent network administrators out there.

My only point with firewalls everyone knows, close all ports, period. What hard about opening a port for credit card traffic with a rule like "allow ip from x to y out established portx" and "deny ip from y to x in portx". Well to that effect anyway.

Section 3 Protecting you against yourself

Although many sites may be locked down, and traffic separated, there still lays a risk of compromise. A smart hack may work part-time for you, helping out to make ends meet during the recession, or just cause it's a quick buck during his college years. As small as computers are getting, he could drop one in on your network and still grab packets. What can be done about these obscure threats? Encrypt traffic from POS systems to Credit Card Terminal systems. Adding services like internal VPN or Stunnel technology would plug up this type of hole. Even if you could not afford to segregate traffic, simply putting this in place would null in void 90% of problems to began with.

Another afterthought on protecting you against you, mission critical, it is a good word to label a credit card terminal. Most cc network terminals are nothing more then software and services installed on windows and UNIX based PC's. It shows fitting that some see this computer as a multimedia device, an Internet terminal, or even an extra computer used for LAN games. During your boring life as a sales associate, playing games on your cell phone, or bringing in a Game Boy can help. But it's this easy to use a device for something other then it's purpose, such as a cell phone, that drives people to this madness. When I questioned my co-worker on why someone would do this he replied "If a normal credit card terminal at the register could play video games, they would install them on it!" I guess this is human nature. My reply STOP IT! Don't waste my time because a virus got on your credit card terminal, because the email told you to run it's attached program. And yes this is the hell that is my day to day routine, like said before, people just don't care, and these things happen.

Part 4 General Points of interest

Section 1 Visa CISP (Cardholder Information Security Program)

Visa CISP Audit guideline is a great place to start when attempting to protect your business from credit card fraud electronically. CISP stands for "Cardholder Information Security Program". It has been in existence for over 2 years, although it has only been fully implemented and followed in recent months. Following basic guidelines that they have provided will surely give you more piece of mind. They have created a "Digital Dozen(tm)" list. This list is their twelve basic steps you can use to protect your credit card network. They are Install and maintain a working firewall, keep patches up-to-date, protect stored data, encrypt data across public networks, use anti-virus software, restrict access, use unique ID's for your users, avoid vendor default passwords, track access to data, have a security audit regularly, have an information security policy, restrict physical access to data.

Now obviously these are all "Duh" remarks, but, remember some of my cases studies. Companies have no regard for these simple to implement systems. Further they are in violation of Visa policy when they do not comply with the "Digital Dozen(tm)" program. So, just setup a security audit, take the time to update service packs, and create unique user ID's. For heaven's sake, get rid of that lynksys route / firewall / WEP / cheese grader!

Section 2 Unavoidable Threats

Although you can do your part, and protect your information to a "T", sometimes this is not enough. F.E.P.'s and ISO's can sometimes be lazy, and not make full checks of your identity. For this reason, basic card terminals are being cloned every day. Sometimes by people who work for these companies, and have full access to merchant information. While the industry is working to get better security in place, there is still no "Great White Hype" as of yet. This is why I am strongly against these terminals. With credit card networks, their is a higher attention to detail with security, and the software is not fully available to the public. Until a more premeditate solution is in place, all you can do is keep close tabs on your bank accounts.

Conclusion

Basically, as long as merchants take their networks from an objective standpoint, and put good procedures in place, they should have nothing to worry about. But, if they do not, watch out, because now they have an army of enlightened soldiers coming after them!

Use last 10 min. for Q/A of credit card networks

References

Notice These resources were used to either assist in creating this paper, or are links to many related topic's. These list are not a complete guild to their parent fields, but more as pointers to 'general' resources.

Security Resources -

Visa CISP Audit
http//www.usa.visa.com/business/merchants/cisp_index.html

World Wide E-Commerce Fraud Prevention Network
http//www.merchantfraudsquad.com/index.html

General On-line Resources -

Flow of credit cards
http//www.usa.visa.com/business/merchants/guide_to_transaction.html?it=h2_/index.html

Transaction World Magazine
http//www.transactionworld.com/

Terminal Resources -

Hypercom
http//www.hypercom.com/

Programming guides to Hypercom terminals
http//www.hypercom.com/products/Download.asp?Nav=66&Nav=65

Verifone
http//www.verifone.com/

Programming guide to Verifone terminals
http//www.verifone.com/pdf/tcl_ref.pdf

Credit Card Network Vendors -

Auric Systems
http//www.auricsystems.com/

CC Bill
http//www.ccbill.com/

CyberSource
http//www.cybersource.com/products_and_services/electronic_payments/

eOne Global
http//www.eoneglobal.com/

Go Software
http//www.pccharge.net/

I4 Commerce
http//www.i4commerce.com/

IC Verify
http//www.icverify.com/

Infinet Incorporated
http//www.infinet-inc.com/qs.asp?page_id=3&site_id=1

Infospace Corporation
http//www.authorize.net/

Paymetric Corporation
http//www.paymetric.com/

Shift4 Corporation
http//www.shift4.com/

UniComp
http//www.unicomp.com/products/software/cambire/about/

Verisign
http//www.verisign.com/products/payflow/pro/index.html/

Front End Processors -

1st Horizon
1st Tennessee
http//www.firsttennessee.com/ft_docs/cfm/biz.cfm?
section=biz&menu=corp_biz&body=corp_merchant_services

5th/3rd Bank
http//www.53.com/

Electronic Clearing House
ECHO
http//www.echo-inc.com/

First Data Corporation
FDC, FDR, Nabanco, Chase, CardNET
http//www.firstdata.com/index.jsp

Global Payment Processing
NDC, MAPP, GPP, MDI
http//www.globalpaymentsinc.com/index2.asp

Nova Processing (not affiliated with Discover/NOVUS)
http//www.novainfo.com/

Paymentech
http//www.paymentech.net/

Vital Processing
VisaNET, Visa
http//www.vitalps.com/

Credit Card Issuer Resources -

American Express
http//www.americanexpress.com/

Diners Club
http//www.dinersclub.com/

Discover Card / Novus
http//www.discovercard.com/

JCB (Japan Credit Bureau) Card
http//www.jcb.co.jp/index2.html

Master Card
http//www.mastercardintl.com/cgi-bin/index.cgi

Visa
http//www.visa.com/

eof