Remedying the Dismal State of the Credit Card System:

A Look at Solutions Past, Present, and Future

Andy Brody

14 May 2007

CS 199r

THEY CAN TAKE MY SOUL BUT THEY CAN'T TAKE MY NAME!
VISA CALLED. SOMEONE STOLE YOUR IDENTITY.
I NEED A NEW BATTLE CRY.
HOW ABOUT "OUCH"?

© Scott Adams, Inc./Dist. by UFS, Inc.

Every few weeks, it seems, another news story breaks about one company or another accidentally leaking credit card and other sensitive information about their customers or employees. The largest, of course, is the recent loss by TJX Cos. of a tremendous amount of sensitive information in the form of credit card, driver's license, and Social Security numbers over a period of many months. Estimates of the goods stolen range from 45 to 200 million credit card numbers (Pereira 2007). This follows the theft of 40 million card numbers from CardSystems in 2005, along with a host of smaller incidents at various organizations. Breaches like these fuel credit card fraud and identity theft, and indeed a growing number of crimes are now being traced back to the TJX incident. These companies in many cases don't actually need to keep the sensitive information, but do so in the name of convenience and profit.

The information finds its way into the hands of criminals in other ways as well, with much of it coming directly from consumers through social engineering attacks or indirectly from them through dumpster diving. Regardless, the issuing banks of the four major credit card associations (VISA, MasterCard, American Express, and Discover) lost $1.24 billion to credit card fraud in 2006 (HSN Consultants 2007). Identity theft or fraud is rampant, with 15 million victims in 2006 according to the Identity Theft Resource Center. However, the credit card associations and their issuing banks are for the most part not tremendously interested in doing much more than they already are. To understand why, one must examine the forces acting on those companies.

The Beast:

The credit card system as it exists today is a multi-headed beast, with each head pulling in somewhat different directions. Because most of the heads involved are corporations, many of those directions are toward the profits of that party. The credit card associations, such as VISA or MasterCard are the most visible part of the system, and are synonymous with the entire structure for many people. These networks take a share of all money traveling through the system and push the liability for risks inherent in the system to the banks and merchants. They give others the responsibility of making sure card users pay their bills and of paying the cost for fraudulent transactions. Still, they do want to encourage banks, merchants, and consumers to participate, so they have developed sophisticated systems over the years to detect fraud in order to minimize losses and assuage the concerns of the other parties. From the network's point of view, this works pretty well at keeping fraud to a manageable level – they're still profitable. Even from the bank's point of view, the fraud is expensive, but so are potential solutions. From the consumer's point of view, on the other hand, incorrectly flagged purchases and unnoticed fraud are constant annoyances. The network is content to have everyone falsely believe the system to be secure so long as it remains profitable.

The financial organizations that issue credit and debit cards to consumers as well as those that provide the card processing services to merchants have motives that are similar to those of the card associations. They want more consumers to use credit cards, and more merchants to accept credit cards. They push the liability for fraud to the merchants when they can (claiming that the merchants failed to take appropriate security measures, for example), but often do bear the cost of fraud. This means that banks have a special interest in improving the overall security of the system, although they would be content to instead raise their charges to cover their costs.

Merchants' motives are also similar, although their customers are consumers, not financial organizations. The merchants accept payment for their goods or services via credit cards in the hopes that this will make purchases more convenient. They want more customers and thus don't want to scare people away by losing their customers' data, although they would very much like to keep any information they can get their hands on if it would help them market their products. It is noteworthy that the merchant really shouldn't need to keep the consumers' financial information – they would probably be perfectly happy to just receive authorization for the transaction from an appropriate party, whether a bank or card association.

The consumers, of course, value convenience very highly. As a highly fractious and individualized group, they don't necessarily act in their own financial best interest. This can be rather problematic, as the other groups are mostly dedicated to making it as easy as possible for the consumers to part with their money. Ultimately, all of the other parties push their costs to the consumers by increasing their charges and raising their prices, so consumers have a large interest in minimizing inefficiency and loss within the system whatever the cause may be.

So why does the situation as a whole seem so dire? How can the financial organizations sit on their haunches while there is so much theft and fraud happening? When it comes down to it, their profits just aren't hurt that much. Although there's an enormous amount of fraud, it's not so large in comparison to the total money spent. "Fraud losses are a cost of doing business, and that cost remains manageable for credit card issuers in the U.S. As long as fraud doesn't go up above 7.0¢ per $100 in volume... issuers will continue to favor customer convenience over security" (HSN Consultants June 2006). The financial institutions also benefit from a "That couldn't happen to me, I'm so careful!" mentality on the part of the consumers that leads them to continue to use credit cards more and more. Individuals are hurt much more by the fraud, whether or not they are themselves victims of it. They deal with the irritation of approving and rejecting purchases, and must trust that the countless organizations holding on to their private information will keep it safe, or else sacrifice the benefits and conveniences that this modern technology can bring.

Past Solutions:

There have actually been several proposals for reforms, some of which have been put into place. The basic signature verification only protects against theft of the physical card, since people making a duplicate card could just sign it themselves. Cashiers rarely check the signature anyway, which John Hargrave of Zug.com demonstrated in dramatic fashion. He signed a receipt at Dunkin Donuts with “KRIS P. KREME,” drew all manner of scribbles and drawings at other stores, pasted a portion of a credit card safety brochure on another receipt, wrote out a song on an extra-secure electronic signature pad, and only had a purchase denied when he signed for three 42-inch plasma TVs with “NOT AUTHORIZED.” He took pictures of all of the receipts while standing at the register, which could have looked suspicious but hardly fazed anyone. Clearly signatures don’t help very much.

The PINs present on debit cards are more commonly verified, but most of the time they aren’t used. The PINs are often stored in plain text at various points in processing, which makes them vulnerable to theft, and in any case they’re not used at all in Internet purchases. A more promising innovation is the inclusion of what VISA calls the Card Verification Value and MasterCard calls the Card Validation Code (others have other Three Letter Acronyms). Extra information is included in the magnetic stripe and used for transactions where the card is present, and a different extra few digits are printed on the back of the card for use in transactions where the card is not present. The networks mandate that no organizations can store these extra bits longer than they have to, although it isn’t clear whether they always actually do so. This would probably reduce fraud significantly except that including these extra bits is optional, and thus not very useful except as a small supplement to the existing fraud-detection systems.

There is one proposed system for Secure Electronic Transactions (SET) that is especially noteworthy. It was developed beginning in 1996 by VISA and MasterCard in collaboration with IBM and a number of other companies to be an open system for conducting business over the Internet. SET uses public key cryptography in the form of X.509 certificates, and would create a sort of public key infrastructure in which all of the different parties in the credit card system are issued their own key pairs. It provides information only to those who need it, so for example the merchant never sees the customer's financial information (which is encrypted with a bank's public key), and the bank never sees what exactly the customer is buying (which is encrypted with the merchant's public key). The whole system is quite secure by virtue of encrypting and authenticating the transfers between the various parties and by virtue of limiting who has access to which pieces of information. No merchant touches a customer's decrypted payment information and thus cannot lose it the way TJX and others have done. It sounds almost too good to be true. Why, then, wasn't it adopted?

SET arrived on the scene a little too soon for it to be well-received. The restrictions at the time on the export of high-strength cryptography led to the use of weak 56-bit key DES encryption in the protocol. DES was widely known to be not terribly secure, and it was well within the power of organizations such as the NSA to build a massively parallel (and expensive) DES cracking machine to decrypt messages on a timescale of around one second (Schneier, 1996). Such a system was not very future-proof given the continual increases in processing power, and even though SET would do its job of protecting against the common credit card thief, it was viewed with suspicion on account of this weakness. SET also introduced a lot of complexity that made the system more difficult for consumers and merchants alike in comparison to competing e-commerce solutions like SSL. The consumers had to download and keep an "eWallet" that contained their key pair as well as the public keys of various organizations, which limited the portability of the system and made it more cumbersome to use. For many, there didn't seem to be any compelling reason to use SET – its security was overkill. "What SET really needs is 'some huge credit-card disaster that costs customers, banks and merchants a lot of money and grabs our attention'" (Morgan, 1999). The disasters didn't arrive until SET was long dead.

Current Solutions:

In the years since, there have been several more modest proposals that show some promise. VISA offers a service called Verified by Visa (similar to MasterCard's SecureCode) that provides a two-factor authentication method. It effectively replaces the CVV/CVC that's printed on the card with some longer, user-specified piece of information such as a password. Password authentication is familiar to users and relatively painless, although it isn't all that secure, especially in comparison to SET. People don't tend to be very good at picking secure passwords, and the actual implementation of Verified by Visa leaves it somewhat open to social engineering attacks that mimic it (Anti-Phishing Working Group, 2004). The system requires additional work for the card issuer, who actually manages the password database, as well as for merchants, who have to update their checkout systems to work Verified by Visa. It's a nice effort, but it doesn't provide such a large improvement in security, especially since it still isn't all that popular with merchants and issuing banks.

There are a number of other systems in the works, some of which seem more viable than others. Dynamic virtual credit card numbers could ensure that the number that is given to merchants is not the real credit card number, but instead a number that is used once or just a few times (Molloy, Li, and Li 2007). It runs into a little bit of trouble with doing this offline because you need some kind of computing device. For this, a Java-enabled phone works quite nicely, as an already widespread mobile computing platform. Cell phone makers would be pleased with anything that ties people more closely to their devices and forces those with aging phones to buy new ones. Still, not everyone would be thrilled by the prospect of a newfangled use for their phones.

VeriSign, RSA, and others have been independently developing similar token-based systems that would generate a one-time-use number. VeriSign's system incorporates the device within a normal-sized credit card, which would make it much more familiar to users. The card would naturally be more expensive than a plain old plastic card, and would also require a supporting infrastructure on the merchant and acquirer's side. It's not clear how durable the things would be, but VeriSign claims they would last two years. If people can get used to the idea, and banks and merchants are willing to upgrade their systems, this would be a significant improvement.

Other companies would like to consolidate the payment services so that fewer parties need to see consumers' personal information. Many merchants make their inventories available through Amazon.com, which both allows Amazon to appear to have a much larger selection of products, and also means that only Amazon need see the customer's credit card information. Both PayPal and Google Checkout provide similar payment services to merchants. As unfortunate it is to be creating huge centralized databases of financial information, the alternative isn't really lots of small databases, but rather lots of databases that are almost as huge. It is perhaps preferable to hand your information over to just Google rather than to every merchant and its Nigerian friends. However, all these services are very expensive for the merchants, who must give a hefty cut of their sales to whichever company they've chosen. The costs are in the end borne by the consumers, as merchants raise their prices to compensate. This consolidation isn't a wonderful solution, but it's better than nothing.

Future Solutions:

So what should we do? Do any of these different ideas make sense? Can they work together? The above proposals are for the most part nice ideas, and will be good measures to take in the short term. However, they don't for the most part change the fundamental flow of information through the system, which means that today's problems will be reduced but not by any means solved. Verified by Visa is vulnerable to phishing, as are the consolidated payment services offered by PayPal and others. Even the systems involving one-time-use numbers are vulnerable to these man in the middle attacks, although much less so because the number can't be reused indefinitely. It is time that the industry looked back at SET, examined why that system failed, and asked itself whether a public key infrastructure deserves a second chance.

Today, strong public key cryptography is widespread in the form of SSL/TLS. Every major browser and operating system ships with keys built in. Although in the past SET may have seemed overkill, we now see a "huge credit card disaster" every few months, and although some institutions can absorb the losses without batting an eye, the system now looks flawed. Adopting a new public key infrastructure would impose significant costs to the merchants, the card issuers, and the card associations, but it really wouldn't demand much more than some of the other proposals. Because it relies on existing technology, there would be no need to develop ever smaller tokens or bring cell phone carriers into the mix. The system would still depend on the old issuing banks to give users their public keys – the parties don't change, only the flow of information between them.

By incorporating the consumer client software within an already ubiquitous product such as a browser or even the operating system itself, getting the system up and running would be relatively easy. In the operating system case, Microsoft doesn't actually have a large stake in this, but they would most likely be happy to be associated with a new secure and open (i.e. not evil) system designed to fix security problems. Other OS makers would take part, not wanting to be outdone. The browser, on the other hand, is a more natural fit for such a system. The browser is already involved in basically all Internet transactions, so distributing the client as an extension or plug-in makes a good deal of sense. The "eWallet" of SET wasn't very popular due to its large size for the time, but Internet users today are much more accustomed to such things (take the ubiquitous Adobe Flash Player, for example). The latest versions of the Internet Explorer, Opera, and Firefox web browsers already include user privacy protections in the form of anti-phishing features, so adding components to fight credit card fraud would be a perfect next step. Firefox's fraud protection began as a third-party extension by Google, which was only later integrated into the main program – the new public key system could do the same thing even if it didn't get the cooperation of the browser makers.

The system would admittedly cost merchants, banks, and networks a good deal to update their storefronts and other infrastructure. On the other hand, the improvement in security would be tremendous, and other systems that wouldn't improve security very much are also costly. The card associations currently classify online transactions in their highest-risk category, which means that merchants pay an additional fee to use it. They could easily spur a new system's adoption by charging merchants less, which would help offset the costs. Furthermore, with this new infrastructure in place, it would be easy to add new smart cards, contactless cards, or any other such physical technology. One of the greatest advantages of a public key system is actually its simplicity: rather than having all these multifarious authentication schemes, a public key system allows many parties to communicate in confidence, transmitting exactly what they want exclusively to the intended recipients. Corporations today seem satisfied with the current way of conducting business, but they would be wise to think twice before angry consumers take matters into their own hands through their representatives in congress.

References

Anti-Phishing Working Group. “VISA – ‘Notice from VISA’” 14 December 2004. Retrieved from <http://www.antiphishing.org/phishing_archive/12-14-04_VISA/12-14-04_VISA.html> on 13 May 2007.

Camp, L. Jean. *Trust and Risk in Internet Commerce*. Cambridge: The MIT Press, 2000.

DeGennaro, Ramon P. “Merchant Acquirers and Payment Card Processors: A Look inside the Black Box.” *Economic Review*. 2006, First Quarter, 27-42.

Electronic Frontier Foundation. “Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design” Sebastopal, CA: O’Reilly, 1998.
see also <http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/>

Gutmann, Peter. “PKI: It’s Not Dead, Just Resting” *Computer*, vol. 35, no. 8, 2002, 41-49.

Hargrave, John. “The Credit Card Prank II” 18 January 2005. Retrieved from <http://www.zug.com/pranks/credit_card/> on 13 May 2007.

HSN Consultants. *The Nilson Report*. No. 858, June 2006.

HSN Consultants. *The Nilson Report*. No. 876, March 2007.

Identity Theft Resource Center. “Facts and Statistics.” 30 April 2007. Retrieved from <http://www.idtheftmostwanted.org/artman2/publish/m_facts/Facts_and_Statistics.shtml> on 13 May 2007.

Jesdanun, Anick. “VeriSign to Offer Passwords on Bank Card.” *Associated Press Online*. 1 May 2007. *LexisNexis* News Wires, retrieved 13 May 2007.

Macdonald, Dunca A. “Data Security Blame Game Solves Nothing.” *American Banker*, vol. 172, no. 76, 2007. 11-11.

Macgregor, Rob. *Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice*. IBM, June 1997. Retrieved from <http://publib-b.boulder.ibm.com/abstracts/sg244978.html?Open> on 13 May 2007.

Molloy, Ian, Jiangtao Li, and Ninghui Li. “Dynamic Virtual Credit Card Numbers.” CERIAS 2007 Symposium. Poster retrieved from <http://www.cerias.purdue.edu/symposium/2007/materials/posters.php#469-BB6>. Paper to be published in *Proceedings of the Eleventh Financial Cryptography Conference*.

Morgan, Cynthia. “Dead Set Against SET?” *Computerworld*, 29 March 1999. Pg. 74.

Pereira, Joseph. “Breaking the Code: How Credit-Card Data Went Out Wireless Door” *Wall*

Street Journal. (Eastern edition). 4 May 2007. pg. A1

Reilly, David. “Secure Electronic Transactions: An Overview” October 1999. Retrieved from <http://www.davidreilly.com/topics/electronic_commerce/essays/secure_electronic_transactions.html> on 13 May 2007.

Schneier, Bruce. *Applied Cryptography*. New York: Wiley, 1996.

US Department of Justice. “Identity Theft and Identity Fraud.” Retrieved from <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html> on 13 May 2007.

Vijayan, Jaikumar. “Debit card fraud outbreak raises questions about data breach.” *Computerworld*, 9 march 2006. Retrieved from <http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=109427> on 13 May 2007.

Visa U.S.A. “Verified by Visa: How It Works.” Retrieved from <http://usa.visa.com/personal/security/visa_security_program/vbv/how_it_works.html> on 13 May 2007.

Wolrath, Carl Eric. “Secure Electronic Transaction: a market survey and a test implementation of SET technology.” 27 September 1998. Retrieved from <http://www.wolrath.com/set.html> on 13 May 2007.