Ending credit card idiocy

Warren D. Smith*
WDSmith@fastmail.fm

February 26, 2003

Abstract — **It is embarrassing for anyone with the slightest exposure to cryptographic algorithms to behold a monetary system as stupid as the present "credit card system." I explain why and explain how to improve it drastically. (Note: the ideas in this paper are mostly not new. Nevertheless it seems worth saying them.)**

Keywords — cryptographic hash functions, smart cards, fraud.

1 Introduction

There has never been a more complicated economy than now. It is ridiculous that this economy runs on "credit cards," which may be the most laughably insecure monetary system ever invented.

In this system, you own a plastic card with a number printed on it. Supposedly the plastic card is hard to forge. Perhaps forgery is beyond the ability of individuals – though I regard even that claim as dubious – but it is obvious that, say, governments (or rival credit card companies) are fully capable of forging them[1]. But it is not necessary to forge, duplicate, or steal the card (which would require effort, and in the latter case, risk) to use it to make illegal fraudulent purchases. It suffices merely to obtain the *number* printed on the card. For example by looking at it, or from videotape, or by listening to phone conversations by use of a cheap, legally purchasable, radio scanner. An article in *The New York Times* [4] claimed somewhere between $\$10^9$-$10^{11}$ of credit card fraud occurs each year, with card numbers being offered for sale over the internet in an criminal "underground economy." (Price: a few dollars.) Every time the card is (legitimately) employed, the number is transmitted from buyer to seller, and then from seller both to the credit card company and to the seller's business records. This causes a vast number of copies of your "secret" number to spread over the world, making eventual theft of that number inevitable[2]. Once having gotten your number, the thief can then use it to make an unboundedly large number of illegal purchases of cars, houses, yachts, etc. A month later, these appear on your bill. But you then can claim those purchases were not *really* made by you, and then refuse to pay the bill, at which point the credit card company eats the cost, and then has to hire investigators to try to track down the thief. Supposedly this is a great "advantage" of the credit card system. But in reality, those investigators may want to investigate *you*, since maybe you invented the "thief." (In which case you may find yourself in a lot of trouble.) And also, of course, ultimately the costs of all this *are* paid by you, or equivalent people, indirectly. Thus this advantage is really merely a grand delusion created by marketers.

All this keeps tremendous numbers of investigators and thieves and marketers happily in business forever. Meanwhile, I refuse to use a credit card due to these risks (and also for independent privacy reasons[3]).

2 A less moronic system

The point of the present paper is that, with today's technology (indeed with 20-year old technology and ideas) it is possible actually to do something sensible instead – easily.

Let your credit card contain an electronic chip. The chip contains inside its ROM, your 512-bit (secret, random) number N. The card is capable of communication with the outside world via an electrical and/or optical interface.

To make a purchase:

1. Apply a "cryptographically secure hash function [2][1]" f to map N to a 128-bit number $A = f(N)$. (A needs to be computed only once.)
2. Similarly map N *and* the current time t (e.g. deciseconds since the beginning of the year 2000 Greenwich Mean Time) *and* the monetary value v of the purchase, to a 128-bit number B.
3. Send the resulting 256 bits (A and B) to the seller, as well as v and t. (All this is done by the chip inside your card.)
4. The seller transmits them to the credit card company.
5. The credit card company uses A and a hash table lookup to deduce your secret number N and confirm (or deny) that you are a valid credit card holder.

*DIMACS, Rutgers, New Brunswick NJ

[1] Airdrops of fake money have been made in wars with the object of destabilizing the enemy's monetary system.

[2] One recent "security innovation" is the use of *encryption* when transmitting the secret number from buyer to seller, so that wiretappers cannot deduce it. This of course has zero effect on everything I just said.

[3] The credit card companies sell your name, and whatever data they can get about you (e.g. what you purchase) to whomever they want, e.g. direct-marketing companies [5]. They also have the power to ruin you at any time by creating "records" showing you are a thief, con-man, or a deadbeat. That could be due either to malicious intent, either on their part, or on the part of somebody complaining about you to them, or it could be due to pure accident. Both have happened. All this is another issue and will not be discussed in this paper – for that see [5].

6. The credit card company uses N and f and the time t and value v to deduce B and (by comparison with the received B) to confirm or deny you just made a legitimate purchase, and to update the accounts of the buyer and seller. (Note, it is impossible to make more than 1 purchase per decisecond.)

Now let us compare this system with the present laughable one. At no time does the seller, nor anybody besides you and the credit card company, ever get your secret number. A wiretapper, with access to the entire transmitted bit stream, remains incapable[4] of using the information thus garnered, to make any purchase if he waits more than a decisecond later and/or if that purchase is for a monetary amount different from v. On the other hand, if the wiretapper tries to make a same-value purchase during the same decisecond (which he *does* have the informational ability to do), then the credit card company instantly refuses to honor either his illegal purchase, or your legal one, and instantly warns you of the theft attempt, and could try to investigate immediately[5].

There is no need for encryption of transmissions, and it now is impossible to forge a credit card a priori.

To "steal your credit card number" it now is necessary to either physically take your card (simply looking at it does not suffice!) – which is risky and difficult (or at least, nontrivial... certainly it is thousands of times harder than simply stealing a number from an ever-accumulating pile of such numbers sitting, in tremendous numbers of copies, essentially in public for years) – or to get the credit card company to provide the number. The latter could be made essentially impossible by the credit card company only storing the numbers in encrypted form, with the decryption keys only known by closely guarded computers and inaccessible by almost all employees and almost all computers at that company. Indeed the decrypted numbers themselves are never needed except as intermediate quantities in a calculation, hence could be held inside dedicated computers which only run one, fairly simple, program ever, which never chooses to make those numbers available to the outside world. Under these circumstances proof that a credit card company had released even *one* secret number would be grounds for a scandal possibly leading to the quick bankruptcy of that company[6].

Even if a thief did physically take your card, then that thief's life still could be made difficult by using, in the protocol, in addition to t and v, biometric or personal information p about the legitimate cardowner. (Examples: eye color, hair color, gender, claimed date of birth, and/or a short secret personal number.) A thief in ignorance of p would be in trouble, and a thief with the wrong gender or eye color, would be unable to make in-person purchases.

A different enhancement of our protocol would involve the seller, before re-transmission to the credit card company, employing encryption via his own private key. This would authenticate that seller and prevent seller-spoofing by wiretappers.

The system I've just described would cut theft by factors of thousands immediately while at the same time being a simpler and easier system to deal with.

References

[1] Ross Anderson & Eli Biham: Tiger: a fast new hash function, `http://www.cs.technion.ac.il/ biham/Reports/Tiger/tiger/tiger.html`

[2] H. Dobbertin, A. Bosselaers, B. Preneel: The hash function RIPEMD-160, `http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html`.

[3] Donn B. Parker: Vulnerabilities of EFTs [electronic funds transfers] to intentionally caused losses, Commun. of the ACM 22,12 (Dec. 1979) 654-660.

[4] Matt Richtel: Credit card theft thrives online as global market, Page 1 of New York Times, 13 May 2002.

[5] J.Rothfeder: Privacy For Sale, Simon and Schuster, New York 1992.

[4] Assuming cryptographic hash functions really are as secure as they are believed to be, and assuming the wiretapper's computational resources are bounded by the amount of computers presently available in the world running for 10^6 years.

[5] By also incorporating the ID# (or a hashed version of it) of the seller, as well ans t and v, into step 2, the thief would be forced to make a same-value purchase, in the same decisecond, from the same seller.

[6] If the credit card company wished to accumulate lots of information about you, with the intent of later selling that information to marketing companies, this would unfortunately still be possible, and still without need for the credit card company to dangerously expose your secret key – all the accumulated information could simply be stored in a hash table indexed by a *hash* of your secret number. Even if this table were easy to access, that would still be fully compatible with making your secret number hard to access.