A Survey of Security in Online Credit Card Payments

Umesh Shankar and Miriam Walker
May, 2001

Credit cards are the primary means of payment for goods and services purchased online. Many characteristics of credit cards leave merchants and banks vulnerable to fraud, inconvenience and, for merchants, loss of customers. We explore the inherent advantages and disadvantages of credit card payments. In response to the limitations of credit cards some challengers to traditional credit card systems have been developed, such as the use of one-time credit card numbers and smart card-enabled credit cards. The advantages and disadvantages of these approaches are discussed.

I. Introduction

By virtually any measure, electronic commerce (e-commerce) is growing rapidly: the Census Bureau estimates that retail e-commerce sales jumped to $8.7 billion in the fourth quarter of 2000, a 67% increase over the period a year earlier[1]. Online transactions are not amenable to many traditional payment methods. Methods that require physical transfer, e.g., cash, money orders, and checks, are impractical. Electronic funds transfers require direct knowledge of the sending and receiving bank accounts, although companies like PayPal[2] and Yahoo[3] are creating their own direct-payment networks to remove this restriction. Credit cards, which are not subject to these restrictions, are the most frequently used payment method, used in about 95% of online transactions[4].

Checks, money orders, and wire transfers are not practical for e-commerce. In the first two cases, the time required to transfer the money is considerable, eliminating the efficiency and convenience of online transactions[5]. Furthermore, none of the three admit a simple, reliable mechanism to stop payment in the event of a dispute, such as when goods are not delivered as ordered. Purchase orders are typically only available to large institutional customers. In the absence of more sophisticated mechanisms for online purchases, individuals use their credit cards. Consumers already have a trust relationship with the banks that issue the cards; infrastructure, electronic and legal, is in place to make the system work relatively consistently. Credit card users are protected by federal legislation that limits individual liability for fraudulent purchases to $50, dramatically

---

[1] "Retail E-Commerce Sales", Census Bureau of the Commerce Department.
http://ww.census.gov/mrts/www/current.html
[2] http://www.paypal.com
[3] http://paydirect.yahoo.com
[4] Enabling Retail Payments on the Internet
14 February 2000
By Kenneth Kerr (Gartner Group)
[5] Qchex is an online check payment system. A check is just an agreement to pay verified only by a signature, and a Qchex check lacks the signature. There are no additional security features and the limited liability guaranteed by credit card companies is not extended to users of the system. The appeal of Qchex may be primarily for exchanging checks with trusted parties. (https://www.qchex.com/benefit.asp.)

lowering the risk to individuals of shopping online; most issuers have a zero-liability policy[6,7].

Credit cards are not the panacea that we might hope for: with the increase in credit card use on the Internet has come a dramatic increase in credit card fraud. For users even to be aware they are being defrauded, they must vigilantly audit their transaction records (typically monthly statements, though real-time online access is common). While the $50 liability limit shields shoppers, the hassle of canceling cards and the feeling of victimization take their toll. Credit cards may be issued to criminals with sufficient information about another individual. The gathering of this information is known as "identity theft." Such problems are difficult to correct and damaged credit histories are common[8]. Credit cards are also, as their name implies, a source of consumer credit, allowing people to make larger purchases than otherwise possible.

The risks associated with credit card use in conventional transactions are exacerbated by the nature of online transactions: first, neither party can be certain of the other's identity; and second, the goods ordered may take some time to be delivered. On delivery, the buyer may discover that the merchandise does not match his expectations. Liability laws and the economic power wielded by the card companies and the issuing banks over merchants reduce the risk to buyers. Losses due to fraud are usually absorbed by merchants, whose burden it is to prevent fraudulent use. These losses are significant for online merchants: many suffer from fraud rates many times higher than traditional retailers, compounding the already higher fees they pay for "card-not-present" credit card transactions (more in "Individual Fraud," below).

One of the impediments to the continued growth of e-commerce is the lack of secure forms of payment; thus, a number of potential solutions to the problem have been developed. We will focus on systems derivative of credit cards, as consumers are more likely to adopt payment methods that are compatible with their current practices. We will attempt to classify the problems associated with the use of ordinary credit cards, survey the approaches currently being deployed to improve the situation, then characterize some likely future developments and propose some additional changes of our own.

II. The Problems

There are several issues associated with online credit card use. Chief among them is fraud, which is perpetrated by both individuals and merchants. Another problem is the lack of security that can lead to the compromise of credit card numbers stored in online databases.

MERCHANT FRAUD

Merchant fraud takes three basic forms: nondelivery, and overcharging, and charges for unwanted goods or services. Nondelivery means that the merchant either does not deliver the goods ordered or does not deliver the correct item. Overcharging involves the merchant charging more than the agreed-upon amount for the correct good

[6] Visa's zero-liability policy: http://www.visa.com/av/zero_liability/main.html
[7] American Express may, at its discretion (following investigation) require payment of up to $50. (Phone conversation with American Express representative.)
[8] FTC Bureau of Consumer Protection site on Identity Theft: http://www.consumer.gov/idtheft/

or service. The latter case involves charging for an unwanted good or service, usually as part of an ongoing scam, where consumers are simply fraudulently billed or duped into paying extra charges[9]. In the case of a genuine mistake, it is usually possible to correct the error; if a merchant is dishonest, typically the credit card company must be brought in to resolve the payment dispute. It is unusual for actual online retailers to commit fraud, as they have the least protection of all involved parties. Most fraud is committed by outfits created for that purpose alone.

INDIVIDUAL FRAUD

Individual fraud on the Internet is a more pervasive problem. First, it is easy for individuals to remain anonymous or to impersonate others. Worse, credit cards were designed to rely on physical signatures for authentication, a mechanism that is rendered useless in e-commerce. In practice, it is difficult for merchants to prevent fraud in the online world, where there are no security cameras or other physical mechanisms to catch criminals after the fact. The purchaser does not have to present a physical card, which may contain additional security features, e.g. additional code numbers, photographs. This type of fraud, in "card-not-present" situations, results in the merchant bearing not only the full cost of the fraudulent purchase, but an additional administrative fee (usually $10-15)[11] imposed by the card networks for the "chargeback". Chargebacks occur in an astonishingly high 2.6% of online purchases[10]; offline purchases typically have chargeback rates many times lower. By contrast, the issuers typically bear full responsibility for card-present purchases with a physical signed receipt, where fraud rates are considerably lower. Compounding retailers' woes, the card networks (Visa, MasterCard, etc.) charge higher per-transaction fees for card-not-present situations to recoup their own losses, e.g., handling complaints and issuing new cards. Online orders, like mail or telephone orders, are subject to fees of 2-3%, compared with rates around 1.5-1.75% for large in-store retailing[11].

Credit cards may be employed to pay for goods and services that may be intangible, such as downloadable software. Simple methods such as comparing the billing and shipping address are not effective when no physical good are being shipped. Nor can the shipping address for gifts be verified. Merchants are reluctant to reject orders and the process of verifying identity is complex and inconclusive. Given that merchants are unable to require all customers to take additional precautions, insecure credit card systems will be supported for a long time into the future, even if verification of identity is stronger with newer systems.

---

[9] FTC site on Consumer Protection for E-Commerce: http://www.ftc.gov/bcp/menu-internet.htm

[10] "Pains and Gains of Online Credit Card Security Schemes "
31 October 2000
By Avivah Litan , John Pescatore (Gartner Group)

[11] Accepting Credit Card Payments on the Internet
Kenneth Kerr
January 24, 2000 (Gartner Group)
http://gartner11.gartnerweb.com/public/static/hotc/hc00085970.html

III. Existing Solutions

There are three classes of methods used for authentication: who you are (thumbprint, retina scan); what you have (tamperproof smart card, keys); what you know (passwords, credit card numbers)[12]. Reliance solely on the latter has led to many of the cases of fraud; determined criminals readily obtain card numbers and addresses. Recent developments have used combinations of two or more methods. Expiration of credentials can also limit risk.

SIMPLE AUTHENTICATION AND DETECTION

Online merchants typically require some additional information to verify credit cards. The most common is the purchaser's billing address, which can be verified against the billing address on record with the issuing bank. Another heuristic is checking to see if the shipping and billing addresses match. This mechanism is supported by most card issuers, as it is relatively low-cost and an effective first-pass deterrent (simple theft of a card does not yield the address).

"SMARTER" CREDIT CARD

American Express' Blue card has a chip embedded in the card itself as well as the traditional magnetic stripe. This chip supposedly enables more secure online transactions. Planned additions include the ability to impersonate other cards and to act as a "smart card", a substitute for cash transactions at places such as vending machines and parking meters[13]. The claim of added security from the card reader is a bit suspect: when using the reader, the authenticity of the card is verified with a digital certificate on the card and a user-supplied PIN[14]. However, it is not clear how this is more secure; the card number still has to go to, and possibly be stored by, the merchant. In all likelihood, the real benefit will be realized when more compelling applications are developed for download onto the chip. More recently, Visa has introduced "smart" Visa cards with substantially the same features. Integration into SET, below, is likely the primary initial purpose[15].

SET AND ITS DERIVATIVES

The Secure Electronic Transaction specification[16], created jointly by Visa and MasterCard, was developed to facilitate secure online transactions. It aimed to solve one of the fundamental underlying problems of e-commerce: lack of authentication. It assigns digital certificates to each participant: consumer, merchant, and banks, using these for mutual authentication at each step. The hierarchy of trust is similar to the PKI (public-key infrastructure) employed by, for example, Secure Socket Layer (SSL). In principle, the substantial verification needed to get a digital certificate is combined with their intrinsic security (they are hard to forge), which makes for a secure system. The primary, and

---

[12] FTC Publication "Authentication and Technology Issues Relating to Access" http://www.ftc.gov/acoas/papers/ati_paper_1.htm

[13] http://www.epinions.com/finc-review-2069-1414F32-38CBCEE0-prod2

[14] http://home4.americanexpress.com/blue/faq_reader.asp?Entry=86

[15] http://www-s2.visa.com/pd/smart/faq.html

[16] http://www.setco.org/download/set_bk1.pdf

obvious, drawback is that additional infrastructure is required at the server and client sides. Indeed, the additional requirements have led to the de facto death of the SET standard. Merchants were unwilling to take the financial risk of implementing the new architecture when they were being offered no reduction in liability. Consumers had no incentive to switch to using new cards and readers since their liability was almost, if not actually, zero.

Visa's follow-up to SET is its Payer Authorization program. This program requires purchasers to use a PIN or password in card-not-present situations[17]. Visa is using its considerable clout to force online merchants to adopt certain security measures[18,19]. The next step is to use a digital certificate on the card combined with a PIN. Visa says that there are about 23 million Visa cards with chips in them[20] (of more than 1 billion total Visa cards); it remains to be seen if their use in this fashion will be widespread.

SINGLE-USE CARD NUMBER

The principle underlying single-use card numbers is that fraud would be reduced if merely stealing a card number were not sufficient to make additional, authorized purchases. These one-time numbers are generated by the bank on behalf of cardholders to be used for a single purchase, after which time the number can not be reused. Cardholders can substitute the single-use number for the number on their physical card and hence keep the physical card number secret from on-line merchants. Given the recent hackings of databases of online merchants[21], many on-line shoppers are wary of disclosing credit card numbers even to trusted merchants. Single-use card numbers provide no additional protection for merchants since the card number does not provide additional verification of the customer's identity, but limits the damage caused by databases being hacked.

Major credit card issuers have been implementing single-use programs in the past year. The most prominent examples are American Express, Discover, and MBNA. American Express' PrivatePayments program[22] allows consumers to obtain single-use numbers from American Express directly to be used for purchases. The numbers expire after a purchase is made or after approximately 30 days from the date of issue. For this reason, the plan cannot be used for recurring or advance-order purchases, or in cases where the number is stored for future transactions. The generated numbers are subject to all the

---

[17] Kurt Thumlert, "Beyond SET: Enhanced Security for Online Transactions": http://www.ecomresourcecenter.com/ecom_connection/0401_3.html

[18] Visa press release "Alliance with Internet Security Systems and new payer authentication service": http://www-s2.visa.com/av/news/press_release.ghtml?pr_form_edit=370

[19] Visa press release "Visa U.S.A. Works with E-Merchants to 'Deadbolt' Their Front Doors to Cardholder Data Online": http://www-s2.visa.com/av/news/press_release.ghtml?pr_form_edit=628&edit_file=

[20] http://www.visa.com/av/press_center/digital/faq.html#smart

[21] **"**Egghead cracked; data at risk": http://www.zdnet.com/zdnn/stories/news/0,4586,2668179,00.html
"Hacker steals huge credit card database":
http://www.cnn.com/2000/TECH/computing/12/13/credit.cards.com.hacked/
"Recent CDuniverse Breach Wasn't Company's First":
http://www.internetnews.com/ec-news/article/0,,4_288801,00.html

[22] American Express website: http://www26.americanexpress.com/privatepayments/info_page.jsp

same restrictions as the original card; there is no way to set transaction limits for each one. Discover and MBNA use technology from Orbiscom. Orbiscom's technology is more sophisticated: users may choose the expiration date and spending limit for each single-use number. The Orbiscom variant associates a generated card number, transaction value and frequency with a single merchant to facilitate recurring purchases.

Both single-use technologies are backwards compatible: generated numbers are indistinguishable from ordinary credit card numbers as far as anyone but the issuing bank is concerned. In each case, however a single account, which is also linked to a traditional card, is used to clear the transactions. Offline transactions still open the possibility for fraud. If the original number is stolen, it may be used for any purchase without any extra restrictions.

FRAUD DETECTION

Perhaps one of the most effective ways of minimizing losses from credit card fraud is not prevention but detection. Banks track the charges that a customer typically makes and contact the customer to verify any extraordinary charges[23]. Given that they have the capability to detect anomalies in individuals' purchase patterns, it makes sense that banks perform this check. Researchers have developed data-mining techniques for detecting patterns of fraud[24]. The cost of such checking is covered by part of the percentage of purchases that the merchant pays to the credit card network. Nonetheless, there is still certainly value in merchant detection of potential fraud before a transaction is consummated (if for no other reason than to lower their own liability). There are many products available to screen purchases for suspicious patterns of activity[25]. When detected, the purchase can be stopped or be subjected to additional verification.

IV. Future Developments

Most emerging solutions, including one-time numbers, smart cards, and direct payments require the user to enter a secret PIN, password, or biometric information. The additional layer of security makes en masse fraud considerably more challenging. Numbers that expire quickly are more difficult to exploit as well; hackers have a small window of time to make fraudulent purchase, usually during the time after the initial theft when they are being most heavily investigated. Cavio has started using thumbprint scans as authentication for business-to-business transactions. Encryption and protection of AMEX Blue and the other "smart" credit card services use possession of the smart card (and the digital certificate encoded thereon) coupled with a PIN or password as authentication.

---

[23] Trust in Cyberspace. Schneider, F. B. (ed) (1999) National Academy Press: Washington D.C

[24] Chan et al., "Distributed Data Mining in Credit Card Fraud Detection", http://cs.fit.edu/~pkc/papers/ieee-is99.pdf

[25] Many commerce server products include this as an optional feature. Some standalone products are available from CrediView (http://www.crediview.com/solution), CyberSource (http://www.cybersource.com/protected_buy), and DCTI (http://www.dcti.com/dcti_merchant_fraud.html).

Since backwards compatibility is paramount (merchants don't want to turn customers away), incremental solutions are important. SET, for example, can be phased in, coexisting with insecure card transactions. Issuing banks can help by encouraging use of the new technologies and phasing out old, insecure forms of authentication. Using one's mother's maiden name as a password is clearly not secure: such information can be determined as a matter of public record from birth certificates. If public-key cryptography is impractical, then the shared secrets (symmetric keys) should be dynamic. Qantas Frequent Flyer programs[26], for example, require the flight numbers and dates for one of the last five flights claimed as the shared secret if the user forgets her PIN. Banks hold the power to make incentives for customers as well as structure the penalty that merchants pay accordingly.

Perhaps business-to-business transactions will drive the changes. Businesses are better positioned to test new methods of payment since they are more likely to have access to technical support.

Apparently detection and prevention in the current system is reasonably effective at keeping down costs to credit card companies. Visa says that "overall card fraud losses have dropped to an all-time low of 0.06% of total transaction volume – or just 6 cents for every $100 in transactions"[27]. However, statistics on e-commerce purchases paints a much bleaker picture, with some merchants claiming that up to 20% of purchases on their sites are fraudulent[28]. As with many statistics related to credit card fraud, it is impossible to know real fraud rates as detection is less than perfect and there is no central and unbiased authority.

Conclusion

There is certainly a need for improved payment methods to combat credit card fraud, but which methods will succeed is uncertain. Backwards compatibility and ease of use for consumers are important to merchants while any methods chosen must appeal to banks, which hold the balance of power. It is hard to evaluate the potential of smart cards, as the promised features have never totally eventuated for cards such as American Express' Blue. And the practical ability of digital certificates to improve security is offset by the inconvenience to merchants and customers. There must be incentives for customers such that all customers use more secure purchase methods and fraud can't be hidden amongst the proportion of purchases using legacy insecure payment methods. Credit card companies are the only group with sufficient power to provide incentives to customers and merchants to increase security – and yet merchants bear the brunt of fraud costs. A new method of secure payment must clearly identify a customer to merchants and guarantee that the customer agrees to pay. Merchants must only be able to charge what the customer agrees to pay for the goods and payment must only be processed if goods

[26] Qantas frequent flyer webpages: https://www.qantas.com.au/fflyer/dyns/fpin
Accessed on 5/5/01.
[27] http://www-s2.visa.com/av/news/press_release.ghtml?pr_form_edit=271&edit_file=
San Francisco, 2/22/2000
[28] http://www.cnn.com/TECH/computing/9903/11/webfraud.idg/

are as ordered. Merchants should not have to pay higher percentages to banks in case of card-not-present transactions and higher volumes and values of purchasing (and particularly higher balances carrying over from month to month) should compensate banks for making such changes.