Chapter 9
Securing Financial Transactions on the Internet

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

Securing payment information on the Internet is challenging work. With proper care, attention to detail, and selection and use of the right tools, e-commerce site administrators can indeed ensure privacy and integrity of data for both their employers and customers alike. Remember that any security solution requires constant attention or it risks becoming a problem in and of itself. Secure payment processing environments rely on careful separation of activities where a “defense in depth” approach can help to shield you from threats coming from the Internet.

INTRODUCTION

Consumer confidence in the security and trustworthiness of business conducted over the Internet is the single most important issue facing electronic commerce today. Internet-based credit card fraud is reaching huge proportions and is driving hundreds of online businesses to the brink of extinction when their merchant banking relationships are terminated due to excessive fraud and chargeback costs. According to the Gartner Group (www.gartner.com), fraud is 12 times higher on the Internet than in the physical world of face-to-face or Mail Order/Phone Order sales. Cybersource (www.cybersource.com) reports that 83 percent of online merchants complain of the problems they experience with fraudulent charges on credit cards.

The Internet is fundamentally changing the way we do business. The traditional ideas of the marketplace and the consumer have morphed into previously unheard of models as technology evolves. The Internet is also changing our concept of money. New online forms of payment come forth regularly. Some of these nontraditional currencies are bringing about new challenges and new rewards to businesses and consumers alike. But, as the saying goes, the more things change, the more they stay the same—criminals exist online just as they do in the physical world, and many of them are working feverishly to beat the system.

DOI: 10.4018/978-1-5225-0273-9.ch009
Securing payment information on the Internet is challenging work, but it is possible (Russell, 2001). With proper care, attention to detail, and selection and use of the right tools, e-commerce site administrators can indeed ensure privacy and integrity of data for both their employers and customers alike. Remember that any security solution requires constant attention or it risks becoming a problem in and of itself.

Because of the nature of Internet sales, it’s impossible to ignore traditional credit cards and their cousins, debit cards and charge cards, wherever e-commerce is conducted. Before looking at ways to bring about an improved online environment of trust and security with payment card data, it’s important to understand some fundamental operating principles and common operating practices to help better define where to focus security efforts.

INTERNET PAYMENT CARD SYSTEMS

With today’s technology of intelligent Point of Sale (POS) devices, high speed communication networks, and hidden back-end host systems, charge processing can appear simple, transparent, and intuitive to the uninitiated, but, in fact, the participant involvement and the steps of processing are far from trivial when you examine the sheer number of systems involved and the high volume of charges (Russell, 2001). The technical complexities stem from the foundation of the equally complex concept of trust.

Credit cards, charge cards, bank cards, payment cards, no matter what you call them, all relate to a family of payment options that involve relationships rooted in trust and good faith. You trust that the financial institution that issued you a card will pay the merchant for the goods and services you purchase. Merchants trust that the card issuers will pay them reasonably quickly, and the card issuers trust that you’ll pay your bill on time each month to reimburse the money they’re advancing on your behalf.

Although they’re often thought by most people to be the same, credit and charge cards differ in how they work and in the agreements associated with each. Many of these payment cards are considerably different from one another in several ways. In general, a credit card represents an account that carries a preset spending limit established by the card issuer, based on a line of credit obtained at the time of issue. Some are signature lines of credit, while others are secured lines of credit, where funds on deposit limit charges and serve as collateral for the credit card in the event of nonpayment of charges.

In addition, their balances against that line of credit may be paid in full or financed over time. As such, finance charges apply to unpaid balances left at the end of the month, at fixed Annual Percentage Rates (APR) that are set at the time of issue and that may or may not change over time. Visa and MasterCard are the most prevalent examples of credit cards issued by specific banks or other financial institutions that license the use of Visa and MasterCard trademarks from the brand associations.

Charge cards, like the American Express Personal (Green), Gold, and Platinum Cards, are not tied to revolving lines of credit—they carry no preset spending limits, are due in full at the end of the month, and do not accumulate interest or finance charges under normal uses. Diners Club and Carte Blanche are two other examples of charge card products.

Debit cards, on the other hand, are tied to a checking account and may be used in place of a check for payment. Once the balance of the underlying checking account is exhausted, requests for payments using the associated debit card will be declined, unless there are other arrangements in place (e.g., overdraft line of credit loans, savings account fund transfers, etc.). These arrangements are usually made before the debit card is issued or may be added anytime while the account is in good standing. Another