Security Features of SellerDeck Web Sites

Introduction

This paper describes the security techniques used by SellerDeck and the possible attacks that might be made. It compares SellerDeck products with comparable common solutions.

Payment Security

SellerDeck allows orders to be placed securely over the Internet. All orders and customer details are encrypted at the web site and then downloaded to a desktop PC before being unencrypted. However, the biggest security issue for ecommerce sites lies around card payment, and for that reason SellerDeck handles these somewhat differently. There are a variety of methods of securing these payments.

PCI DSS Compliance

Since 30th June 2007, all organisations that store, process or transmit credit card payments have been required to comply with the Payment Card Industry Data Security Standard (PCI DSS) which is a mandatory standard agreed by all of the banks, Mastercard and Visa. Failing to comply can lead to withdrawal of merchant status and unlimited fines.

The 12-point standard imposes stringent requirements in areas such as physical and electronic security and encryption. Many of these are complicated and expensive to fulfill, and beyond the means of most smaller businesses. For more information about PCI DSS, download the PCI Quick Reference Guide from www.pcisecuritystandards.org.

Payment service providers (PSPs)

There are two major disadvantages of taking card numbers for payment at your web site. The first is that you must be PCI DSS compliant as explained above. To properly implement this standard will cost, at a minimum, tens of thousands of pounds. The second disadvantage is that you will be storing card data, and therefore become a potential target for hacking attacks. Unfortunately this is no longer just a theoretical possibility and there are highly skilled criminal gangs operating that specifically target web sites with card data available.

For this reason SellerDeck recommend that all merchants use a Payment Service Provider (PSP) such as SellerDeck Payments (which is highly integrated with our software), Paypal or Worldpay. In this case, payment security and PCI DSS compliance is handled by the service provider.

Historic methods of capturing payment details used by SellerDeck include a Java applet that performs encryption at the buyers desktop; a shared SSL service from SellerDeck; and capturing card details directly at the merchant web site under an SSL certificate. Although encryption is used in all of these

cases, and SellerDeck have no knowledge of ever suffering a breach of security in this area, SellerDeck no longer recommends these methods because they are not PCI DSS compliant.

SSL

Secure Socket Layer (SSL) was the industry-standard method for securing online payments for a number of years. It is still a requirement for companies that want to achieve independent compliance with PCI DSS. When the web site is secured using SSL, the http: prefix of the site address is replaced by https:, and a 'golden padlock' is displayed in the visitor's browser.

If a third party payment system is in use, SSL is not required; but SSL can optionally be used by SellerDeck to secure the other checkout pages where customer name and address is gathered. The advantages of having your own SSL certificate are:

- you can capture name and address under SSL. On a fairly busy site, it's probably the case that this will more than pay for the cost of the certificate in additional orders
- a potential security warning when returning from the PSP page is avoided. You get this with all PSPs when the browser is set to warn when transitioning from SSL to non-SSL pages. Although by the time the warning is displayed, the payment has already been successfully processed, it still avoids potential concern on the part of customers

SellerDeck isn't designed to work with any PSP where the card details are actually captured on the merchant's site. This is because the hosting, web site etc would all need to be fully PCI DSS compliant (expensive and difficult), and capturing cards in this way also invites attack.

Logged on Customers

The account and password details for customers logging on to an SellerDeck-driven store are also protected. Passwords are not stored on the web site, nor are they ever sent across the Internet. SellerDeck derives a signature using an MD5 (signature) of the password, so it is designed to be completely secure. Only this signature (from which you cannot derive the original password) is stored on the web site and sent from the buyer to the web site. The logon process also takes advantage of SSL to provide additional protection whenever an SSL certificate is enabled at the web site.

Possible attacks

All security methods can be attacked. The design objective was to ensure that using SellerDeck to take orders across the Net was at worst no more risky than other accepted methods of accepting credit card orders, and that SellerDeck's inherent security was at least as good as that of SSL. We will briefly discuss the main routes for attack and how SellerDeck products deal with them:

Merchant site to PSP

When the merchant site forwards the buyer to the PSP through their browser, it passes all relevant details to the PSP using URL parameters. An unscrupulous buyer could intercept this call and change the parameter for the payment amount. However, if tampering can happen and were to occur resulting in a lower amount being paid, the order would show up in SellerDeck's order processing as "part paid" (correctly). However, if digital download was being used, the buyer would already have got the goods at a bargain price. SellerDeck Payments and other PSPs prevent this scam using a variety of different security methods, including digital signatures that ensure the message comes

from the merchant site and has not been tampered with. When these measures are in place, the wrong amount cannot be paid.

PSP to merchant site

When the payment has successfully been processed, the PSP calls the merchant site to indicate a successful payment. An unscrupulous buyer can attempt to "spoof" this callback by entering a callback URL into their browser, while not completing the payment at the PSP site. This would mean that the merchant site would think that a successful payment had been made when it hadn't. Digital goods would be supplied to the buyer without payment, and physical goods might also be shipped unless each payment was checked against the PSP's own records, a laborious task. SellerDeck Payments and other PSPs prevent this scam using a variety of different security methods, including digital signatures that ensure the message comes from the PSP and has not been tampered with. When these measures are in place, callbacks to the merchant site that are not correctly signed are discarded.

Interception of packets on the web

If an SSL certificate is used, all aspects of orders placed using SellerDeck software are totally secure against this threat - all data is only transmitted once it has been encrypted. If a PSP is used, with or without SSL, no payment data appears unencrypted in transit on the Internet. In practice, interception of packets on the web is a remote possibility in any case. Nearly all hacking takes place at the web site, where SellerDeck holds the data in encrypted form.

Breaking security on the web site enabling hackers to copy web orders.

SellerDeck security is particularly good in this respect. Other methods, including some SSLonly based systems, keep orders on the web server in clear text. With SellerDeck, orders are still encrypted whether SSL is used or not, and the typical haul will be much smaller than with an SSL server because orders are always removed from the web site when the vendor downloads them. Employees at an Internet Service Provider (ISP) have access to the servers. They could easily copy stored orders both silently and transparently. They can also remove any potential audit trail. If ISP employees are disaffected, this is a serious risk with most current ecommerce systems. SellerDeck prevents this abuse since all orders are held encrypted.

Physical breach of security at the vendor site.

This is a known and accepted risk as it is the same risk as where credit card slips are physically stored at the vendor's site. Anyone who keeps client details on any form of PC (or even on paper records) is vulnerable, which is why SellerDeck recommend use of a PSP. However, SellerDeck has an option to encrypt card data on the desktop and the password to decrypt the data is not stored, only becoming available when a user is logged on and derived from their password. This represents a high level of security.

Network access to the PC at the vendor site.

Most business PCs now use a broadband connection and are therefore permanently connected to the internet. This represents an increased risk compared with the intermittent dial-up connections that were in use a few years ago. It is essential that every PC or network is protected by a good firewall to prevent unauthorised access from outside; and by anti- virus and anti-spyware software to prevent compromise of the PC.

Subversion of the web site to substitute different software

Substituting software at the web site is a potential risk. For a hacker to subvert SellerDeck security would require complete disassembly and understanding of the security method - a reasonably uncommon skill. There is a clear audit trail of this type of attack which is itself a disincentive.

Timing attacks

This is only theoretically an avenue of attack. The concept behind it is that timing the encryption process gives some indication of the size of key used - a large number takes more processing time than a small one. This is used to try and limit the universe of potential keys for a brute-force attack. In practice, it is useless on the Internet because: a) The net itself introduces random delay b) Some of the encryption is performed on the client's PC. Since these will vary enormously in specification and loading, no useful information can be obtained. A similar argument applies to encryption at the server c) The encryption at the client cannot easily be observed or timed d) For client-based encryption, the encryption is only performed once per PC so would not yield any comparisons

Technical Information

SellerDeck uses the following encryption and digital signature technologies.

Diffie-Hellman

Diffie-Hellman key exchange has been published for over 25 years and has been proved to be strong. RSA have based their encryption method on the same fundamental mathematics.
RSA (used in SSL) is essentially a derivation of Diffie- Hellman. SellerDeck chose to use Diffie-Hellman for the following reasons: it is a public / private key method, which is essential for the ordering model adopted by SellerDeck; the algorithm has been around for many years and has stood the test of time; it is now patent-free; it has been selected by an increasing number of industry leaders as their system of choice, including Microsoft, Sun Microsystems for their SKIP system, and Cisco for their routers.

The encryption technique used falls into two parts. The first is to use Diffie-Hellman key exchange (see below) to agree an up to 128 bit key which is then used by a SAFER block cipher. The Diffie-Hellman key used is up to 1024 bits, depending on performance. This encryption method is used on the following fields only : credit card number credit card type credit card expiry date Other fields in orders placed using the system are also encrypted using Safer with a up to 128 bit key, but using a fixed key built in to the software and common across all instances of the software.

Safer

SellerDeck has adopted the SAFER SK-128 block encryption method developed by Massey (the developer of IDEA which is used in PGP). The key for use with SAFER is negotiated using Diffie-Hellman. The algorithm has been around for some time and has stood the test of time. It is a public algorithm and is freely available.

MD5

SellerDeck uses MD5 for digital signatures, including when communicating with payments service providers. Again, the algorithm has been around for some time and has stood the test of time and is a public algorithm which is freely available.

Key length

SellerDeck have adopted a 128 bit Safer key, which gives a reasonable performance whilst being several orders of magnitude beyond where brute force methods could break the encryption. SSL offers generally lower levels. To put things in context, each additional bit of key space
takes twice as long to break. So a 41 bit key is twice as strong as a 40 bit key. The 128 bit key used in SellerDeck products is 4,722,366,482,869,645,213,696 times as strong as an SSL 56 bit key.

Summary

The combination of SellerDeck with a PCI DSS-compliant payment gateway provides a very high level of security, and ensures that the critical risk, the theft of card payment data, is completely eliminated.