Security

ACTINIC

Introduction

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

Security method

Actinic allows orders to be placed and sent over the Internet. Encryption can be disabled for non-sensitive orders eg requests for further information about a house advertised for sale. If encryption is enabled, it can happen in one of two ways : using SSL or using a Java Applet. An alternative is where all secure payment information is collected by an payment service provider such as NetBanx, Authorize.net, WorldPay, Secure Trading or SECPay. In this case, the security is provided by these companies. This particular option will not be considered further in this paper.

Using SSL encryption

There are two ways of using SSL – where you have your own certificate and where you share a certificate with other people – "Shared SSL". Where either SSL option is used, the buyer's crucial details such as credit card information is sent from the browser to the server using industry standard SSL encryption. At the server, the order is encrypted before being written to disk using the encryption method explained below. Hence all orders are encrypted at all times while they are stored on the web site. When the vendor downloads the orders, they are sent over the Internet using SSL and then decrypted on their PC. Hence there is no large store of orders available online to invite attack.

Decryption is carried out on the vendor's PC after orders have been downloaded from the web.

The encryption technique used falls into two parts. The first is to use Diffie-Hellman key exchange 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.

Using the Actinic Java Applet

If the security method selected is the Actinic inbuilt encryption, then encryption occurs on the buyer's PC and like with SSL, decryption only occurs on the vendor's PC. At no stage is the transaction decrypted whilst it travels over the Internet, or

while it is stored on a web site. In addition, orders (including credit card details) are only stored on a web site until the vendor downloads them to their PC. Again, there is no large store of orders available online to invite attack.

The encryption is carried out by using a Java applet in the browser and is unchanged at the web site. Otherwise encryption and decryption is as described in the section on SSL.
The Java applet is subject to the standard security restrictions of their "sandbox" which restricts their ability to communicate across the Net to only the web site that they are downloaded from.

The following banks have approved their customers use of Actinic Java applet encryption: Barclays Bank, HSBC and The Royal Bank of Scotland.

Logged on Customers

The account and password details for logged on customers are also protected. Passwords aren't stored on the web site, nor are they ever sent across the Internet. Actinic 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.

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. Actinic chose to use Diffie-Hellman for the following reasons :
it is a public / private key method : this is essential for the ordering model adopted by Actinic
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:
Microsoft
Sun Microsystems for their SKIP system
Cisco for their routers

Safer

Actinic 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

Actinic 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

Actinic 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 Actinic products is 4,722,366,482,869,645,213,696 times as strong as an SSL 56 bit key.

Possible attacks

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

Interception of packets on the web

Orders placed using Actinic software are totally secure against this threat - all data is only transmitted once it has been encrypted. No data appears in clear on the Internet in transit. In practise, interception of packets on the web is now a remote possibility.

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

Actinic security is particularly good in this respect. Other methods, including some SSL-only based systems keep orders on the web server in clear text. With Actinic, the hacker would gain no benefit as orders are still encrypted whether SSL is used or not, and the typical haul will be much smaller than with an SSL server as orders are always removed from the web site when the vendor next dials in.

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. Actinic 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.

Network access to the PC at the vendor site.

The vendor's PC is attached by dial-up and therefore not permanently attached. Hence, beyond standard security features provided by the ISP and the PC software, the principal protection is anonymity - there is no way for a hacker to know the identification of the PC with Actinic software running, or when they will be online. SSL based solutions have a server permanently connected to the Internet and keep all

the credit card details available on-line. They are far more vulnerable to compromise in this respect.

Subversion of the web site to substitute different software

Substituting software at the web site is a potential risk. For a hacker to subvert Actinic security they would need to compromise either the encryption at the web site or the Java applet.
a) Compromise of the encryption at the web site at a secure server. This would require complete disassembly and understanding of the security method - a reasonably uncommon skill. There is a clear audit trial of this type of attack which is itself a disincentive.
b) Substitution of the Java Applet. The resulting Java Applet could still only communicate back to its host web site so this method would require a co-operating process running on the web server and would thus leave a clear audit trail. This would require complete disassembly and understanding of the security method - a reasonably uncommon skill, and especially difficult as Actinic have obfuscated their Java Applet (deliberately renamed variables etc. so that it is extremely hard to understand the code).
This risk is far more severe for SSL-only systems which store orders permanently on the web site. If a hacker can get in to a web server, then they can grab all the orders (including historical orders) on the site which are stored in clear text. This is more likely than an attack on Actinic as it would reap a larger reward in terms of credit card information and would leave less of an audit trail and it could happen from any site.

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

Summary

Overall, it can be seen that Actinic represent a much safer way of transacting business across the Internet than just using SSL and this applies whether using SSL or the Actinic Java Applet. This is primarily because they never decrypt the orders at the web site nor store them in clear and this is by far the most likely point of attack.