
SSL or 3DES for IP POS Transactions

Posted by DBorgs - 2005/04/25 20:36

I'm trying to figure out what is the best security solution to deploy for using POS terminals over the Internet. I have had several people tell me about different options to secure the transaction, the first is to encrypt the track 2 data at the terminal and decrypt it on the host using a 3DES algorithm and the other method is to build an SSL client to reside inside the POS.

Each method has its advantage and disadvantages:

3DES

Advantages

- Fast as there is no key to exchange to start the transaction

Disadvantage

- Only part of message encrypted

SSL

Advantages

- The Whole message is encrypted
- Based on http/s or socket

Disadvantage

- Slow, as SSL requires the security key to be exchanged before a transaction is sent
- SSL complex to configure

I want to hear from someone that has gone through this and could let me know what they learnt from their experience.

Bye

=====

SSL or 3DES for IP POS Transactions

Posted by smsshift4 - 2005/07/06 20:32

The short answer is you need both or something equivalent. SSL is designed to protect data while it is in transit over the Internet or any LAN/WAN. 3DES would be required to store the data in the terminal.

In your pro's and con's you mentioned a con that SSL is difficult to configure but failed to mention a con about a secure 3DES key management.

Technically, SSL is an asymmetric encryption algorithm meaning that the key used to encrypt is different than the key used for decryption (referred to as a public key & private key). This method by definition means that the key is not a security risk as no data will be compromised should a hacker have his/her hands on the public key.

3DES on the other hand is a symmetric encryption algorithm meaning that the key used to encrypt is the same key used for decryption. This method means that your data is only as secure as your protection of the key. The problem is that the terminal needs the key to encrypt the data so you're caught in a catch-22. Tackling this problem is not a simple task.

If I have time, I'll try to add more later on this topic.

=====