Securing Credit Card Data

Posted At : December 22, 2005 5:49 PM | Posted By : Mark Kruger
Related Categories: Security

> CF Muse Reader Shane Asks:
> Hey mark, I'm a frequent visitor to your blog. I'm curious what precautions I should take when dealing with storing credit cards in a MSSQL2000DB. I've done plenty of e-commerce solutions, but haven't done one where I need to store the CC's for many years. I know things have changed. Do I need to encrypt these? If so, what methods do you recommend?

Well this is a huge can of worms. In early 2004 (if memory serves) Visa required all its merchants above a certain threshold that sell on-line to be "certified" as "CISP" (Cardholder Info Security Program) compliant. Non-Categorized merchants - which may be defined as merchants with less than 6,000 transactions a year, no "hack" attempts (pretty vague) and who are not on Visa's radar - have avoided the cost of auditing by keeping a low profile while visa has other fish to fry - but the free pass may be coming to an end. Since "level 1" merchants are anyone that Visa says they are, they can require you to submit to an audit (at your expense) in order to continue processing Visa transactions. Wait.. it gets suckier....

If you are identified as "level 1" you must have an annual onsite security assessment by a crony... er.. company certified by Visa. You also must have your network *scanned quarterly* by an independent scan vendor. The cost of these changes is enough to make you flock to Paypal.

What's on the checklist

What does it take to "get certified"? The following items are on the checklist. Much of this is "network" related so you may need to talk to your provider unless you host your own.

- *Build and Maintain a Secure Network* - This could mean a lot of things. Visa is secure, NASA more secure and DOD *very* secure. Visa apparently means a Firewall and no "vendor supplied defaults" for passwords. Surprisingly this still ranks near the top on the list of security no nos. The other day I was trying to re-configure my wireless router and it wouldn't let me in, so I tried the default password and I got in. The first thing I did was change the password (naturally) - right before I realized I was connected to *somebody else's router*. Was I red in the face....
- *Protect Cardholder Data* - This means protect stored data from unauthorized access and encrypt the transmission of cardholder data across the Internet. Note: encryption in the database is NOT a requirement. This is talking about always using SSL for web based transactions.
- *maintain a vulnerability management Program* - "My name is Mark and I'm an insensitive jerk... it's been 2 years since I last criticized my wife's choice of shoes...." No, that's not what it means. It means to scan for viruses and maintain your definitions and "develop and maintain secure systems". That last one is pretty wide open to interpretation.
- *Implement Strong Access Control measures* - This means "need to know" data dissemination, independent logins for network access (no shared logins) and restricted *physical* access to cardholder data. Presumably it means you can't host

your ecommerce site on your laptop at Kinkos.
- *Regularly Monitor and Test Networks* - This is referring to an audit trail of access to Cardholder data, and a test of the security systems and processes (again pretty generic).
- *Maintain a Security Policy* - This means you have a document stored somewhere in your office that is out of date the instant it was completed.

What is interestingly absent from this list is encrypted data. The only mention of encryption has to do with ensuring the *transmission* of data was encrypted.

Personal Take

In my opinion you should *not* choose to store the Credit Card Number in the database unless you have a reoccurring charge - a subscription service. Simply require folks to re-enter that bit each time they purchase from you. If you *do* choose to store the CC data you should follow the guidelines above (within reason) - even if you are not subject to an audit. Personally, in my view the credit card number should always be stored as encrypted in the DB, and it should never be visible or unencrypted until the time comes to create a transaction. Moreover I would also use the CVV2 value and encrypt that as well. Since it is a check bit of the number and the exp date against a key value (generated by Visa) it is a valuable bit of information - arguably more valuable than the exp. date.

To encrypt I think I would shy away from cfencrypt in favor of one of the many Java based CF tags found on **CF Lib.org**. I'm sure that on CFMX the cfencrypt tag is safer than it was on CF 5. But since I've been avoiding it for years now, why stop.

One final note, you can also encrypt the network packets to and from your SQL server using built in net libraries. While this is doable it slows down your connection considerably in my experience. If your DB server and Web server are on the same network this might be overkill. If they are not on the same network (not a good idea but sometimes necessary) then I would recommend a hardware solution like 2 pix routers with point to point 3DES. This keeps you out of the business of managing encryption as well as all the other stuff you have to look after on your SQL server.

Resources
Visa CISP Compliance
Merchant Categories