Webmaniacs - Cryptography and Dentistry

Posted At : May 23, 2008 1:20 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security, Conferences

On Tuesday I took in a workshop on Cryptography by **Dean Saxe**. Dean is an impressive character with a head stuffed full of knowledge and spilling out everywhere. He obviously knew what he was talking about. As a topic, cryptography is so impossibly complicated and intricate that he could not do it justice in a 50 minute session. Most discussions about cryptography center around keys, algorithms and best practices - and this was no exception. Dean recommended against relying on CF's own encrypt and decrypt functions for anything but the most rudimentary encryption. In fact, he probably didn't even go that far. That tidbit of advice is common from almost every security pro I have ever heard mention the subject. When it came to discussing keys it was like a trip to the dentist.

The discussion of keys and secure storage was a dizzying array of circular decision making. Where do I store the keys? Are the keys themselves safe? Are the keys encrypted? Where do I store the keys to unencrypt the keys I have stored? How do I secure those keys? If tweedle beetles battle with paddles in a bottle on a noodle eating poodle in a puddle, would that be a poodle puddle noodle bottle tweedle beetle paddle battle (Thank you Dr. Seuss)? It seems we are all doomed eventually to have a post-it note password stuck to the underside of our desk. I could not help but think of the puzzle penguin made of wood I had as a child - each penguin containing another smaller penguin.

In any case, after some discussion of hardware solutions and the Java keystore tool, Dean's final suggestion was, and I quote:

> *"My best advice regarding encryption is.... don't use it. It complicates things."*

Now, to be fair, Dean was talking about the encryption of credit card numbers and he was recommending using a gateway service provider rather than attempting to store them yourself. Of course, this is precisely the advice we give all of our ecommerce clients - do not store credit card numbers anywhere on your system if you can possibly help it.

It only struck me as funny because it seemed like the concluding sentence of the presentation, as in "Hey this stuff is really really hard and complicated so don't go there if you can help it." As a final salvo to an audience straining to learn about encryption it took the wind out of our sails a bit.

In a perfect world we would all have fancy pants DOD encryption where an armed marine stands guard over our keys in a vault that no one but Nicolas Cage could possibly penetrate. But I don't think that the daunting challenges of PCI compliance should keep us from doing things like encrypting passwords (for example). I suspect that Dean would agree with me.

Sometimes discussing encryption causes us to throw up our hands because it seems there are dangers, insecurities and vulnerabilities around every turn. No solution seems both secure and manageable. My view (with PCI compliance as an exception needing additional attention) is that encryption is another obstacle in a layered defense. Sure, in an easily managed, unobtrusive form it's imperfect. I think the basic question for

most projects is the risk and cost question - how secure do we *have* to be and how secure can we *afford* to be. So keep hashing those passwords and don't let the insecurity of your algorithm deter you (at least not until you can afford an armed marine).

Finally, let me say that I thought the presentation was excellent and I picked up a number of nuances on cryptography of which I was previously unaware. If you need someone to review your system for PCI compliance I'd say Dean would be a great choice.