Herding Cats:
Corned-Beef PCI DSS

January 2010

BrandenWilliams
SECURE BUSINESS GROWTH

Do we have to ask how relevant PCI DSS is to today's information security professional? Definitely relevant enough to have an entire issue dedicated to it! There are societies based on payment security, PCI DSS groups for assessors, victims—I MEAN merchants and service providers—financial institutions, and industry or verticals. You can't look too far without running into some internal project tied to a PCI DSS initiative.

As many have pointed out, PCI DSS is NOT perfect. At its core, it is based on existing standards (such as ISO 27002) with some unique twists designed to combat perceived threats to the security of the payment system. Companies that equate PCI DSS to an information security program will leave gaping holes in their overall security posture, and miss out on excellent opportunities to build upon the baseline that PCI DSS may provide to an organization that implements it.

Data protection is the key to information security, and PCI DSS is no different. I've written in the past (in this publication even) about the healing power of secure hashes, in both as more of a catch-all solution as well as a strategic point solution. My first pieces on hashing discussed using them to comply with PCI DSS, but ignored some of the security implications that you must consider. My later ones concentrated on the RIGHT approach and strategy for doing it.

Luther Martin at Voltage discusses one of the two main issues with hashing in a blog post entitled "How to be PCI compliant yet weak[1];" the ability to create rainbow tables whereby you can easily take a known hash value and look up the input value used to create it. Granted, one of the issues for cardholder data is the limited key space[2] in which card numbers are valid. Remember, all valid PANs start with published six digit BINs[3] and must pass a Luhn check.

Hashing can be much more effective in protecting cardholder data when a "salt" is used. Salts are akin to a password or encryption key for hashing, but implemented in a different manner. Let's say that you have a card number, 4111111111111111, and you want to create a hash of this value. A straight MD5 hash would yield the value "fe745cd9e5facbc7951a700008a69bc1". Now, add the phrase "StayClassySanDiego" to the beginning of that value and you get a completely different output of "1997aba33a8b1f0336df73be6c8d7e61"[4]. Notice how the hashed values are completely different and totally unrelated.

It's still possible to build rainbow tables if you know the salt, but without that knowledge you will not be able to (in a feasible time frame) build your rainbow table, thus making the hash stronger.

The main difference between hashing and encryption is the ability to mathematically go from ciphertext to plaintext with the appropriate key. Encryption enables you to do this while hashing does not. So if you are hashing and then destroying your initial input (i.e., in this case, the PAN), you have no way to change your hashing method if some part of it is disclosed, like the salt. For comparison sake only, consider the salt for a hash and the key for encryption to be equals, then realize that because you are destroying your plaintext, you can NEVER change your keys when you hash!

FOOTNOTES

[1] *Read it here: http://j.mp/8SLhKF*

[2] *http://en.wikipedia.org/wiki/Key_space*

[3] *Here is a good guide: http://j.mp/69Rzj8*

[4] *Some argue that putting the salt at the end will put stronger security around the hashed value.*

Hashing is not dead, but it needs to be used in the appropriate manner. Knowing that a PAN is valid is certainly one big step to earning the ability to use the payment instrument in the system, but you still need more information. Most online retailers require at least an address verification check before approving the purchase. Therefore, a hashed value by itself with some basic transactional data—such as the amount purchased—is much less valuable than a hashed value in the same table as the cardholder’s personal information.

If you choose to use hashing as part of your data protection strategy, just remember its constraints and think carefully about where to deploy it. Remember that compliance does not equal security! Be sure that anything you implement measures up appropriately to both facets of this often misunderstood dichotomy.

Contact information for requests for permission to reproduce or distribute materials available through this course are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.