Cryptographic Algorithms for the Payment Card Industry

Fiona Pattinson, atsec information security

November, 2009, Revised, October 2010

This discussion focuses on the review of encryption mechanisms by Qualified Security Assessors during their assessments of merchants, service providers and the payment applications which are employed within the industry.

NIST operate a program, the Cryptographic Algorithm Validation Program, or CAVP, for validating that those encryption algorithms and security functions approved as FIPS or recommended by NIST are in fact implemented correctly. This is a laudable check to make since NIST determined that around 25% of the algorithm implementations they tested were in fact not implemented correctly and therefore potentially worse than useless for protecting sensitive data[1]. The CAVP website can be found on the NIST's Computer Security Resource Center website[2].

It is probably worth pointing out that we are not talking about the intrinsic strength of the algorithm itself. For example how much effort it takes to brute-force AES or Triple DES. Rather we note the possibility that a programmer, while coding an algorithm into a software application makes some often simple, mistake. The resulting “encryption” that occurs is not a true implementation of the defined algorithm, but is in fact some much weaker function that can be more-easily decoded and that fails to adequately protect the information. If NIST’s statistics are to believed then this is something that happens on a regular basis.

---

[1] NIST. , *ITL NEWSLETTER FOR AUGUST 2006*, [Online], Available from: <http://www.itl.nist.gov/lab/pub/newsaug06.htm>.

[2] http://csrc.nist.gov/groups/STM/cavp/index.html

The PCI SSC have also defined the term “strong cryptography in their glossary[3] as *“Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or “one way”). SHA-1 is an example of an industry-tested and accepted hashing algorithm. Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher). See NIST Special Publication 800-57 (http://csrc.nist.gov/publications/) for more information.”*

The NIST Special Publication, cited by the PCI SSC in their definition, provides background information and establishes frameworks to support appropriate decisions when selecting and using cryptographic mechanisms and recommends conformance testing under the NIST program. It specifies the use of FIPS Approved and NIST recommended algorithms and functions to provide strong cryptography, certainly within the U.S., and is also widely referenced by other nations.

One frequently asked question is in regard topic and encryption is the ability to reduce the scope of the cardholder data environment through the use of encryption. The PCI SSC's response to this question is given in their FAQ available as "FAQ item 10359: *Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS*?"[4] Their response indirectly references NIST's SP 800-57[5] as an example of best practices and of course emphasizes that proper key management is indeed key to the success of encryption

Cryptographic techniques play a significant role in PCI compliance. This of course includes not just encryption, but also the specification of hashing and tokenization (as well as masking) as specified techniques for achieving confidentiality of the PAN data.

The PCI DSS V2.0 specifies the use of cryptography and key management in several places, most noticeably in Requirement 3: “Protect stored cardholder data.” This states that “*Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails*.” and according to the PA-DSS ,which is used by PCI approved assessors to determine compliance of payment applications to the mandated standards, the scope of the PA-DSS review should include the encryption mechanisms used.

As promised in their FAQ mentioned above the PCI SSC have been and continue to study the topic of encryption. Their first document, "Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance,"[6] has been published in October of 2010. In this paper again the tactic of reducing the scope of a PCI DSS assessment through eliminating and consolidating the unnecessary storage of card holder data; carefully architected network segmentation minimizing the number of system components that have access to cardholder data; and using encryption appropriately. The report highlights on this topic that "Encryption solutions are only as good as the industry-approved algorithms and key management practices used, including security controls surrounding the encryption/decryption keys (“Keys”).

---

[3] https://www.pcisecuritystandards.org/security_standards/documents.php
[4] http://selfservice.talisma.com/article.aspx?article=10359&p=81
[5] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
[6] https://www.pcisecuritystandards.org/pdfs/pci_ptp_encryption.pdf

Those responsible for implementing cryptography in a PCI cardholder data environment, as well as responsible payment application vendors will check the implementation correctness of any algorithms or security functions used. Specifying "FIPS Approved mode" in applications and devices in the CDE will support this by ensuring that validated cryptographic algorithms and functions are used. As we have shown, it is not enough to specify an algorithm, key size and other parameters, it is important to ensure that it is also implemented correctly.

For those with in-house developing and implementing algorithms an excellent way to do this is through the NIST Cryptographic Program itself. An accredited laboratory will assist in testing the algorithm or security function implementation and when successfully tested and the results have been validated by NIST, the implementation can optionally appear on the public NIST algorithm validation list [7]

More information about the CAVP scheme, including the official validation lists, can be found at the NIST CAVP website and a list of accredited laboratories[8] providing the testing service is also provided.

For algorithms that are not covered by the validation program but that your QSA may still consider as strong, or allow in conjunction with compensating controls, some assurance to developers and the users of algorithms implementation correctness can be also be gained by having a third party analysis of the implementation correctness of algorithms performed. Some of the better laboratories will also offer an independent review of implementations of other algorithms such as RC4, CRCs, single DES, MAC, Blowfish and others.

[7] http://csrc.nist.gov/groups/STM/cavp/validation.html

[8] http://csrc.nist.gov/groups/STM/testing_labs/index.html