Why and How to Get Cryptographic Modules FIPS Validated

Yi Mao

Date 2012-06-11

Version 1.0

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

The modern information and communication technologies (ICT), using computers connected through networks, are increasingly embedded in many aspects of our daily lives. It brings us the convenience of working from home, e-banking, e-commerce, as well as many public services accessible online. Meanwhile, it also demands the protection of sensitive information against unauthorized access or fraudulent changes. Failure of safe-guarding sensitive information may cause devastating financial and reputational damages to the involved organizations and individuals.

Among a variety of information security approaches to build the defense in depth, cryptography is at the foundation of all information security. Cryptography addresses the prime concerns of confidentiality, authentication, non-repudiation, and data integrity. Symmetric algorithms, such as AES and Triple-DES, are confidentiality measures that prevent the unauthorized disclosure of information to unauthorized individuals or processes by encrypting data during transmission or while in storage. Asymmetric algorithms, such as RSA and DSA, use digital certificates for authentication and digital signatures for both non-repudiation and data integrity. Secure hashing algorithms are used to protect data integrity. Random number generation algorithms provide unpredictable initial vectors or key materials for other cryptographic algorithms mentioned above.

All cryptographic solutions to information security are based on the principle of secure by design, as opposed to security by obfuscation. National Institute of Standards and Technology (NIST) publishes all of the approved cryptographic algorithms coupled with a validation program (CAVP) (http://csrc.nist.gov/groups/STM/cavp/index.html). Anyone can learn, say, how AES works from the published standard FIPS 197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf). Understanding exactly how AES works will not help an attacker to break the encryption. In fact, the more people understand AES and use it properly, the better. Cryptography has become increasingly mathematical in nature. Each NIST approved cryptographic algorithm has been proposed, reviewed, and justified for its correctness and efficiency by top notch mathematicians worldwide. Approved algorithms don't get to stay valid forever. NIST plans ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. NIST SP 800-131A (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf) provides guidance for transitions to stronger cryptographic keys and more robust algorithms.

Although developers are not obligated to adopt NIST approved cryptographic algorithms and have the freedom to invent their own ways of protecting sensitive information, it is wise to take advantage of NIST publications, guidance, and recommendations on cryptographic matters that are freely available on its website. The reason is apparent: Considering the current decompilation and reserve engineering techniques, there is little chance to hide the operation secrecy in the program. Once the home-grown "clever algorithms" consisting of a few rounds of XOR and bits-shifting get revealed from the source code, the sensitive information that is protected by the false sense of security is now open for any attack. Obfuscating the source code may make it more difficult to read off the secrets from the code after decompilation, but it is not a show stopper and only requires a little more persistence to overcome it. Using NIST approved algorithms is beneficial to developers because they will not have to worry about keeping the design of algorithms a secret, which is a huge burden to take on, with a slim chance of success.

Adopting the NIST approved algorithms in place of the vendor proprietary cryptographic solutions is a good start. Nevertheless, the full benefits of using approved algorithms are not realized until the algorithm implementations are validated through the CAVP. Because the implementations from different vendors vary largely due to different programming languages used, different platforms for execution, or different optimization techniques involved, it often happens that the implementations are error-prone regardless of the fact that the algorithm specifications and pseudo code are in the public domain. CAVP metrics have shown that approximately 25% of algorithm implementations are not correct upon their first validation attempt. Our lab's experience confirms this statistic. Validation testing for algorithms under the CAVP is intended to informally verify the correctness of the algorithm implementations. All of the algorithm tests are handled by third-party laboratories. atsec information security is one of the Cryptographic and Security Testing (CST) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) that provides algorithm testing services (http://www.atsec.com/us/cryptographic-algorithm-testing-lab.html). We have a tool used for testing that is provided by CAVP only to the accredited laboratories. It generates the test vectors as inputs to the algorithm implementations, as well as compares the results collected against the correct answers.

Due to the open security of approved cryptographic algorithms, the security strengths they provide solely rely on the length and secrecy of the Cryptographic Sensitive Parameters (e.g., key materials, initial vectors, seeds, salts, etc.) that the algorithms take as inputs. Implementing the approved algorithms and passing the algorithm validation tests is necessary but not sufficient. If the CSPs are not well protected or well generated to start with, things can still go very wrong. Often under the pressure of a tight release schedule or lack of resource, developers unfortunately tend to adopt quick and dirty solutions by hiding keys in the source code or taking short cuts to generate CSPs. The hardcoded keys in the source code are susceptible to reverse engineering and decompilation. Easily predictable keys will become the weakest link of the cryptographic system and substantially reduce the security strength of the entire system. This is where NIST Cryptographic Module Validation Program (CMVP) to the rescue. The cryptography that is not validated by CMVP is viewed by NIST as providing no protection to the information or data – in effect the data would be considered unprotected plaintext.

CMVP validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 (http://csrc.nist.gov/publications/fips/fips140-

2/fips1402.pdf) and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The primary goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules. It serves equally well as a market differentiator and assurance indicator to benefit non-government customers all over the world whose daily work and life heavily depend upon the valuable data that are expected to have the protection under cryptography. According to the CMVP statistics, nearly half of all cryptographic modules tested were found to have flaws in either design or implementation. Validated cryptographic modules not only qualify for sales to U.S. and Canada government agencies, but also signal to other potential customers that they been designed and implemented to meet strong security requirements.

FIPS 140-2 covers eleven areas related to the secure design and implementation of a cryptographic module. Among the eleven areas, emphasis is placed on the cryptographic key management. The standard and its companion Implementation Guidance (http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf) provides detailed requirements and explanations on key generation/establishment, key enter/exit, key storage/destruction, key access under physical and logical protection, and so on. The standard and its IG point to a series of NIST special publications for the recommended methods of establishing/deriving/protecting keys (e.g., SP 800-56, SP 800-57, SP 800-132, SP 800-135, etc.). To understand FIPS 140-2 and the interrelated other cryptographic standards is not a trivial task. Because these standards reflect the most advanced research results in cryptography, as well as the best industry practices, it’s worth the effort of looking into them. The developers of the cryptographic modules that we have validated commented that it is quite educational to get familiar with the standards. To be compliant with FIPS 140-2 has actually helped them to build better products. Had they been equipped with the knowledge of cryptography based standards, they would have stayed away from crafting their own seemingly clever but flawed solutions. In addition, developers tend to produce quality code if they are told in advance that their code will be reviewed by a third party.

On the flip side, the FIPS 140-2 certification program is sometimes criticized for the time and monetary cost associated to the validation endeavors. Inevitably there is cost involved to pay for the CMVP processing fee and lab’s testing effort. This is analogical to visiting a physician’s office for an annual health check-up. It costs some money and time to pay a visit, but the physician identifies the potential problems and provides suggestions on corrective actions to ensure that one’s health system works in the way as expected. This can potentially save the patient in the future from racking up large bills, and even their life, by preventing or postponing severe health problems from occurring. For the same reason, having an accredited CST lab independently validate the module by reviewing its design and implementation, testing its functionality, assessing its vulnerabilities and checking its development life-cycle provides the benefits that are likely to outweigh the validation cost. The gained benefits include, but not limited to, the following:

(1) Modules that have undergone the CMVP validation provide cryptographically sound protections over sensitive data.
(2) Modules that have achieved FIPS 140-2 certification differentiate themselves from competing products due to their assured quality through an independent third-party.
(3) Vendors who take up the challenge of having their products tested under an open standard demonstrate their commitment to security and their dedication to perfect their products, which in turn helps them to build up a good reputation and gain the customers' trust.
(4) Due to the widely recognized merit of FIPS 140-2 certification, the standard itself is also evolving to be an international standard under ISO/IEC FDIS 19790. Vendors with the FIPS 140-2 validation experience are well positioned to quickly advance to meet the requirements from the international standard for cryptographic modules. This surely helps vendors to penetrate and gain the international market.

The validation cost is proportional to the test scope and the initial quality of the cryptographic module. Poorly designed modules with a lot of nonconformities found during the lab's review and testing cycles tend to be costly, and take longer to go through the validation process. It goes without saying that developers will have to fix all of the identified issues and sometimes may need to reengineer the module to a large extent in order to meet the standard requirements. Nevertheless, the cost can be minimized by interweaving the validation process with the module development process. The planning phase of a module development is a good time to get developers trained on the FIPS 140-2 requirements so that the module is designed to be compliant. atsec CST lab provides on-demand FIPS 140-2 training at our facility or on-site at customer's location (http://www.atsec.com/us/fips-140-2-testing.html) throughout the year. The training can take anywhere between one to a few days depending on how deeper into the crypto-world the audience would like to explore. It can also be tailored to meet the specific needs raised from a particular module development. Our experience shows that modules designed and implemented by FIPS 140-2 aware brains pass the conformity test faster and with ease. The investment in training may break even to the savings gained from the development with few error-and-trial cycles and from the reduced validation cost as well.

Although the cryptographic algorithm implementation testing under CAVP is an integral part of the module validation, algorithm certifications can also be achieved independently to the module validation. The algorithm testing mostly uses the black-box approach. The source code review is not required, with very few exceptions, such as AES counter mode. Thus, algorithm validation can be conducted in a fairly short time frame, if the implementation is ready for testing. Some vendors have achieved the algorithm certificates through the atsec CST lab in only a week or two. If the module is designed and built upon a proper understanding of the relationship between the algorithm test and module validation, then it’s feasible to obtain algorithm implementation certificates which may be reused towards the future follow-up module validation. Vendors who have temporary budget constraints could pursue algorithm certifications as the first milestone step and commit to the module certification at a later time when more resources become available.

CAVP and CMVP publish and maintain lists of validated algorithms and modules on the NIST website (e.g., http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html, http://csrc.nist.gov/groups/STM/cmvp/validation.html#01). These programs have gone a long way to guide the proper use of cryptography for information security. FIPS validated products have a better chance to overcome the constant rise of security threats. The consumer demands, not limited from the government agencies, are the ultimate reason for the existence and growth of these validation programs. Whoever takes advantage of working from home and/or using e-banking, e-commerce, and many other online services should challenge their service providers to have their cryptographic components FIPS validated. Without the assurance provided by the validation programs that the cryptographic components in use follow a series of open and rigorous cryptography-based standards to ensure the integrity and security of data, the convenience is overshadowed by the risks. FIPS validation is not a silver bullet in providing the information security, but it is one layer of solid defense in cryptography. The consumers of the modern information and communication technologies, which pretty much include everyone nowadays, will continue to benefit from using FIPS validated products, even if just for their peace of mind.