Experiences with the FIPS

and the FIPS 140-2 Certification Process

Independent Security Evaluators
www.securityevaluators.com

April 15, 2007

1 Introduction

For over a decade all software and hardware cryptographic modules used by the United States government to protect unclassified data have had to pass a vigorous certification process known as the Cryptographic Module Validation Program (CMVP) [3], established by the National Institute for Standards and Technology (NIST). This program is designed to verify that a cryptographic module does indeed meet the requirements specified in a series of documents known as the Federal Information Processing Standard 140 (FIPS-140) [2]. These documents describe in detail the requirements for the module's design, implementation, testing and accompanying documentation. They provide a framework for bestowing upon a module a specific level of security (of which there are four) in 11 distinct categories.

Though the certification process is presented in a (somewhat) understandable and explanatory manner, and though hundreds of products have become FIPS-certified in the past, the process itself often seems daunting and unapproachable by smaller businesses with generally smaller budgets as well as larger corporations with little experience developing government-certified modules. The result is that cryptographic modules being developed for this purpose fall victim to the process itself, and corporations suffer unnecessary financial burdens or the inability to complete the process entirely.

This white paper describes our experiences with the FIPS certification process, from the standpoint of a security consulting firm assisting other companies to generally secure thier products as they undergoe the FIPS certification process and the CMVP.

2 Its not impossible

First, it is helpful to realize that completing the FIPS certification process and CMVP is not an impossible task, and it is not only for large corporations with massive development teams. The process is straightforward, and with a little guidance even very small companies can develop products that could pass the certification test.

There are a number of NIST accredited laboratories known as Cryptographic Module Testing (CMT) laboratories that provide this very service, and it is very helpful (as well as required) to use such services. Each of the thirteen such laboratories have passed the National Voluntary Laboratory Accreditation Program and can assist a business with obtaining FIPS certification. Having prior experience with the certification process allows these laboratories to offer an easy to follow and structured schedule to move forward with the CMVP. Small businesses can work directly with one or more consultants to get direct feedback and advice on how to most effectively achieve the highest level of certification possible.

A larger hurdle a company may face is the time and money resources that must be invested in to the process. The third-party accreditation laboratory will come with a fee, as will the basic certification certificate itself. However the real cost endured by a company is the investment in time. The process can take several months, and add a significant number of man hours as overhead to the development lifetime of a project, including testing, documentation writing, and redesign of the product itself.

It is most helpful though, to realize that these additional costs in overhead are generally necessary to any product's development life cycle and are typically considered good practices. The burden falls heaviest on companies that don't employ these best practices in the first place. Still, even a company with a tried and true development process will inevitably come across additional tasks and overhead costs not normally associated with the development process.

3 The Ground Level

When incorporating the requirements for FIPS certification into a product's design, it is important to begin as early as possible in the development lifecycle. Any engineer or software developer will tell you that changing a requirement, design element, or even a single feature late in the development process is extremely difficult. If you treat the development process as having five stages (design, specification, implementation, testing and maintainence) it is often said to be a factor of 10 times harder to fix a flaw from a previous stage once the next stage is underway. That is, a design flaw discovered in the design phase that would take 15 minutes to remedy typically

costs 2.5 hours once specification has begun, 25 hours once implementation is underway, 250 hours during testing, and can cost as much as 2500 man hours once a system is deployed.

Incorporating the requirements for a FIPS-certified system will almost always require some amount of fundamental changes to be made to a product's design. These requirements do include featurettes that could be simple to implement and test, but risking the need for a fundamental design change could wind up being 100 times more expensive per hour of redesign that is necessary.

It is often a bad habit of developers and engineers, especially in small business settings, to hack up or mangle products late in the process to make fundamental design changes to their products. The hope is that these modifications can get the job done without requiring going back to square-one and redesigning, respecifying, reimplementing or restesting. In addition to being a bad practice, throwing the development process to the wind is not as readily possible during the CVMP. The accredited CMT laboratories will require updated and accurate design documentation, and if deep in the evaluation process could require rechecking large amounts of documentation or implementation. Instead, bring the CMT laboraties into the process during the design phase or specification phase at the latest. This way, required design elements such as a well defined finite state machine, distinct module boundaries, inputs and outputs, proper roles for users, valid error reporting mechanism, etc, can all be built in from the beginning.

The CVMP is intended to validate the development process as well as the final product that is being certified. Hence, the procedure closely mimics the development lifecycle itself. First reviewing the design documentation of the product, then specifics about APIs or other inputs and outputs to the system, followed by an evaluation of the implementation itself, and finally signing off on test results. To incorporate the CVMP early in a product's design not only saves on the cost of man hours, but the CMT laboratories can work in parallel with the developers and engineers building the product such that the overall timeline is not much longer than the development timeline itself. That is, the results of each phase of development can be validated and signed off on by the laboratory while the next phase is underway.

4 Modularity

It is also very helpful to design any product to undergo the CMVP in a way such that all functionality to be validated is modular and capable of being abstracted from the overall product itself. Developers should consider placing all cryptographic functionality in a separate cryptographic module. Then, it is much simpler to certify only the cryptographic module rather than the entire product. Extending the boundries of the certified module to include the entire product and not just the cryptographic module is also not a difficult matter at this point.

In general, modularity is a good approach to any sort of development process. Modules can be developed independently of each other and brought together in the end. By modularizing the validated system-to-be, the cryptographic module can be studied intensy while the remainder of the product can be developed separately altogether. This decreases the overall timeline of the process since niether the development of the product nor the progress of the CMT laboratories block on one another.

Another helpful artifact of designing a moduler product, is that versioning of individual modules or cryptographic algorithms is possible. When one needs to be updated, it simpler to review and recertify that portion than to recertify the entire module. For example, if a previously validated device incorporates 2 modes for encryption, each with a separate cryptographic algorithm, and a 3rd is added, if the other algorithm sub-modules have not changed, in many cases they will not need to be reviewed again before recertification, only the new additional module would need to undergo this process. Therefore is it very important to maintain a good, detailed versioning system that is well documented for the ease of recertification.

5 Additional Security Evaluation

One other aspect of the FIPS certification process that should be brought to the attention of developers and investors alike, is that FIPS 140-2 certification does not imply strong or sound security. In otherwords, having this stamp of approval does not come close to a garauntee that the security of a product is sufficient. Instead it is prudent

and necessary to have an external security-centric evaluation of a product for locating vulnerabilities and design flaws that the CMVP does not identify.

There are many cases left unchecked by the CMT laboratories, such as the presence of buffer overflows, the misuse of cryptographic algorithms in a manner that makes them weaker, the misuse of the product itself, or basically any other security issue not relating to tamper resistance or specific cryptographic algorithms.

For example, FIPS certification can verify that all data encrypted by a device uses a valid encryption algorithm that always produces the correct result, but it does not verify finer details such as whether the device ever reuses an encryption initialization vector, or whether data is hashed and then encrypted when it should be encrypted and then hashed.

For more information on this topic, see [1], the publication produced by Independent Security Evaluators describing several more detailed examples of how the FIPS certification process does not provide sufficient security garauntees.

In short, all products that provide a security component, whether certified or not should receive some sort of security evaluation by an independent 3rd party. There are numerous benefits to this activity, including having new eyes critic the choices made in designing a product, catching security flaws or vulnerabilities that would not ordinarily be brought to the forefront by the CMVP, other certifcation processes or by stand alone analysis tools, and most importantly the advice and input from industry experts in helping to design secure products.

References

[1] INDEPENDENT SECURITY EVALUATORS. Title to be decided, April 2007.

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Fips pub 140-2, 2002.

[3] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Cryptographic module validation program. http://csrc.nist.gov/cryptval/, April 2007.