Implementation issues with FIPS-140

Matthew Gillen (matthew.gillen@rtx.com), Jathan Manley (jathan.manley@rtx.com)

Raytheon BBN Technologies

Submitted in response to Call for Position Papers: Software Supply Chain: Executive Order, Area 2.

The US DoD took major steps toward securing their supply chain with the adoption of NIST-800-171[1] as a baseline set of security controls that all contractors are expected to implement. NIST-800-171 covers a broad range of security controls, and many of the guidelines are practical and good security hygiene. Assuming that the government is looking at the some of the DoD's DFARS clauses as a potential model to expand to all federal contracts, we believe there is one issue in particular that needs significant scrutiny. This paper will focus on one particular control, because it has numerous implementation issues that have not been addressed by US DoD yet. The requirement in NIST-800-171 that this paper will focus on is as follows:

> *3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.*

This requirement doesn't actually say which FIPS standard, but that is clarified in the glossary within the assessment guide NIST-800-171A[2]:

> *FIPS-validated cryptography: A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended).*

This paper makes no claims about the efficacy of FIPS-140 or CMVP to solve the problems they were designed to solve. Specifically, for the purposes of this paper we will assume that the CMVP process produces trusted cryptographic implementations. This paper instead focuses on the larger context in which these cryptographic functions operate, the marketplace within which federal contractors have to operate, and how internet-based protocols like TLS make FIPS-140 compliance a practical impossibility.

There are two classes of problems when it comes to contractors implementing this as a requirement.

Vendor Marketplace

Cryptographic implementation is highly specialized, and the idea behind FIPS-140 to give those implementations intense scrutiny is generally a good idea. What CMVP validates though is the smallest aspect that makes sense, which is typically done as separable library that will be used by applications. However, the linkage between the validated library and the larger application is something typically only the vendor can attest to. Furthermore, FIPS-140 involves more than just the cryptographic implementations, and so major vendors like Microsoft have a "FIPS mode" for their operating system that sets a wide range of options beyond enforcing that the crypto implementations are using the validated module. This wide range of configurations is so detrimental to other operational aspects of maintaining systems that in 2014 Microsoft published a technical note[3] that argued essentially that the only reason to turn "FIPS mode" on is compliance.

There is an important footnote to both the Microsoft Windows and the RedHat Enterprise FIPS configuration options, which is that setting operating-system-wide defaults is just that. Since crypto

operations are done within applications, application code can necessarily provide their own (non-compliant) implementations. It is impossible to enforce FIPS compliance from the operating system level. Instead, each application that uses crypto would have to be audited to ensure that it is both linking to the certified implementation library, and that it is using that library in a complaint manner.

Quote from reference #3:

> *Further, FIPS mode does not and cannot ensure that applications even use encryption at all when appropriate. There is nothing Windows can do to prevent an application from saving plaintext passwords or other sensitive data in unprotected files or registry values. The bottom line here is that just because a software product works when FIPS mode is enabled does not mean that it adheres to government standards.*

The last point with respect to the marketplace is that the FIPS certification can lag the software release significantly. As of this writing, the latest CMVP certificate available[4] for Microsoft Windows 10 is for version 1809. Version 1909 has been out for over a year. This is not a critique of Microsoft, the CMVP process takes a long time. The problem is federal contractors have to do something in the meantime, and both have no idea when a certification might appear for the latest release, nor do they have the means to pursue certification themselves (most contractors are not privy to Microsoft's proprietary source code).

Internet transport protection for business to business information flow

The second major issue is the meaning of FIPS compliance when it comes to internet protocols like TLS. FIPS-140 makes the most sense when there is a self-contained system doing the encryption and decryption, such as with a self-encrypting disk drive, or a networking tunnel that traverses untrusted internet and has dedicated encryptor devices at both ends that are controlled by the same organization. However, when it comes to offering web services on the general internet, you are necessarily interacting with other organizations. To achieve the goal of fully validated cryptography, you would need both the client (web browsers) and servers to be using validated crypto. Mainstream web browsers in use throughout the commercial sector either have no option for FIPS compliance or the options for FIPS-validated crypto are so arcane that no one uses them. To compound the problem, TLS as a protocol has no mechanism for validating that the "other side" is using FIPS validated crypto (e.g. a server can't know if the client connecting to it is using FIPS validated implementations).

Conclusion

The problems that FIPS-140 is looking to solve are important, but the current software development practices and the marketplace realities put severe limitations on how contractors can deploy FIPS compliant software. We believe that achieving the goal of trusted cryptographic implementations requires a framework that is flexible enough to be responsive to zero day exploits and keep pace with frequent update cycles. The ability for contractors and agencies to validate the compliance/configuration of a product's use of trusted cryptographic implementations is critical.

References

1. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
2. https://csrc.nist.gov/publications/detail/sp/800-171a/final
3. https://techcommunity.microsoft.com/t5/microsoft-security-baselines/why-we-8217-re-not-recommending-8220-fips-mode-8221-anymore/ba-p/701037
4. https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation