From:	Kerman, Sara J. (Fed)
To:	chad.boutin@nist.gov
Cc:	Marron, Jeffrey A. (Fed); Foti, James (Fed)
Subject:	CSD Weekly WERB Update
Date:	Thursday, December 20, 2018 12:42:00 PM

Hi Chad,
Two items started the WERB process this week:

NISTIR 8240 Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process (PUB #927303)

Authors: Dustin Moody + multiple other NIST staff

Abstract The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public- key cryptography standards will specify one or more additional digital signature, public-key encryption, and key-establishment algorithms to augment FIPS 186-4, Digital Signature Standard (DSS), as well as special publications SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers. In November 2017, 82 candidate algorithms were submitted to NIST for consideration. Among these, 69 met both the minimum acceptance criteria and our submission requirements, and were accepted as First-Round Candidates on Dec. 20, 2017, marking the beginning of the First Round of the NIST Post-Quantum Cryptography Standardization Process. This report describes the evaluation criteria and selection process, based on public feedback and internal review of the first-round candidates, and summarizes the 26 candidate algorithms announced on January 10, 2019 for moving forward to the second round of the competition. The 17 Second-Round Candidate public-key encryption and key-establishment algorithms are BIKE, Classic McEliece, CRYSTALS- KYBER, FrodoKEM, HQC, LAC, LEDAcrypt (merger of LEDAkem/LEDApkc), NewHope, NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM), NTRU Prime, NTS-KEM, ROLLO (merger of LAKE/LOCKER/Ouroboros-R), Round5 (merger of Hila5/Round2), RQC, SABER, SIKE, and Three Bears. The 9 Second Round Candidates for digital signatures are CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow, and SPHINCS+.

Conference Paper: Determining Forensic Data Requirements for Detecting Hypervisor Attacks (PUB #927335)

Authors: Liu, Changwei; **Singhal, Anoop;** Chandramouli, Ramaswamy; Wijesekera, Duminda;

Fifteenth IFIP 11.9 International Conference on Digital Forensics

Abstract: Hardware/Server virtualization is a key feature of data centers used for cloud computing services and enterprise computing that enables ubiquitous access to shared system resources. Server virtualization is typically performed by a hypervisor, which provides mechanisms to abstract hardware and system resources from an operating system. However, hypervisors are complex software systems with many lines of code and known to have vulnerabilities. This paper analyzes the recent vulnerabilities associated with two open- source hypervisors Xen and KVM as reported by the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) and develops a profile of those vulnerabilities in terms of hypervisor functionality, attack type, and attack source. Based on the predominant number of vulnerabilities in a hypervisor functionality (attack vector), two sample attacks using those attack vectors were launched to exploit those vulnerabilities and to determine the forensic data requirements.

Hope you have a good holiday and a Happy New Year!
Sara