Cryptographic Performance and Certification

The core philosophy of Bonafeyed's data defined security is to secure data before it is placed "in-use" and when retrieved must be viewable by authorized users in the "clear". This is accomplished by deploying a security engine on user's endpoint devices. To be effective, the cryptographic algorithm must provide strong encryption, have lightweight computational demands, low latency operations, and be capable of running on any device no matter the available computing resources. Bonafeyed's answer is the Cy4Secure end-point security engine. Although this security engine can utilize any crypto algorithm, by default it supports both a standard symmetric block cipher and an innovative stream cipher. The block cipher is the Advanced Encryption Standard or AES 256-bit. The stream cipher is a Mersenne Twister (MT) based algorithm employing an 800-bit key and executes using very fast bit-wise exclusive OR (XOR) mathematical operations. XOR operations are natively supported at the core level of modern CPUs allowing the MT algorithm to be easily implemented in higher level languages. Bonafeyed's software development kit includes the Cy4Secure security engine as a plugin for browsers or a code module supporting many operating systems and programming languages including JavaScript, C, Swift, and others. This allows data defined security on a wide range of devices including desktops, laptops, tablets, smartphones, and virtual machines or containers.

When compared to the AES block cipher, the Cy4Secure MT algorithm is faster, uses a large linear-feedback shift register with lower compute requirements, and has a larger cipher block table than AES256. The performance difference is easily seen. Using an 800-bit key for the Mersenne Twister cipher and 256-bit key for AES running on an Intel Xeon X5690 operating at 3.46GHz and 32GB of memory produced the following performance comparisons:

Encrypting 1,000,000 times on 128-byte dataset:

- Cy4Secure operations: 7.526155 seconds
- AES256 operations: 33.473791 seconds

Encrypting 1,000 times on 1MB dataset:

- Cy4Secure took 10.274421 seconds to execute
- AES256 took 227.630874 seconds to execute

Off-the-shelf C code and standard compiling optimizations was used for the performance tests. The results show Cy4Secure's MT based stream cipher is up to 22 times faster than AES256. This advantage introduces the ability to protect all database fields without impacting users' experience and to deploy on any end-point device no matter the computing capacity.

As with all cryptographic modules, they must meet various security requirements including the National Institute of Standards and Technology (NIST) FIPS 140-2, a U.S. government computer security standard. The following is the results running FIPS 140-2 part 1 tests on 1MB data:

- Monobit test - passed
- Poker test - passed
- Runs test – passed

Finally, the Cy4Secure implementation utilizes a patented improvement to the cipher key stream generation (#9,246,681). Keys are generated with a hardware device and validated prior to being accepted for use.

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.