Security concerns dominate the news recently, with continual reports of data breaches, industrial-strength hacking, and widespread malicious software. That bothers encryption code developers like Leah Thompson at wolfSSL, because solutions exist to win these battles. “We currently secure over 1 billion endpoints with our wolfSSL library,” she said, speaking of their celebrated security solution. “Our coverage ranges from the Internet of Things to large-scale server environments, so we encourage more developers to consider us.”

Sure, people still write their passwords on sticky notes attached to their monitors; that’s a different challenge from the one Thompson is solving. Offering end-to-end security solutions, wolfSSL supports encryption on the biggest servers powered by Intel® Xeon® and Intel® Core™ processors all the way down to IoT devices running on Intel® Quark™, Intel® Atom™, or Intel® Arduino* processors.

Just recently, Thompson and her team optimized the wolfSSL Transport Layer Security (TLS) library on 5th generation Intel® Core™ processors. With the inclusion of Intel’s extended instructions, developers can use the wolfSSL libraries for applications on many devices, including embedded technologies. The resulting improvements mean end users will see enhanced speed and security—with reduced power consumption—across a wide range of devices.

Now is certainly the time to act. According to a June 2015 report from the Online Trust Alliance, IoT websites are among the most likely to fail tests for data security and privacy. “The results of this audit serve as a wake-up call to IoT companies that are handling highly sensitive, dynamic, and personal data,” said Craig Spiezle, executive director and president of OTA. “In rushing their products to market without first addressing critical data management and privacy practices, they are putting consumers at risk and inviting regulatory oversight.”

Founded in 2004, wolfSSL initially focused on creating the first open source, dual-licensed embedded Secure Socket Layer (SSL) library. Their alternative to OpenSSL was more portable,
smaller, and faster. It came with a modern API and offered commercial-style developer support. MySQL® soon adopted wolfSSL, and today the company has expanded from its Montana roots to offices in Washington and Oregon.

To fuel further growth, wolfSSL continues in a fast, lean tradition, embracing new technology as needed. According to Thompson, when they recently optimized the Advanced Encryption Standard (AES) instruction set for the 5th generation Intel Core processors, they beefed up what’s known as Bit Manipulation Instructions (BMI). This is a boost for asymmetric cryptography, allowing for math optimizations on large integers up to 1024 bits long. To handle math at this bit size, coders must break down the problem into smaller pieces. There are new instructions in wolfSSL that help optimize those breakdowns and sub-computations.

wolfSSL benchmarks show the wolfSSL secure hash algorithms are now significantly faster. The Advanced Vector Extensions perform multiple word operations with a single instruction (in parallel) to provide this boost in speed. wolfSSL also integrated a high-quality, high-performance entropy source and random number generator. And it includes AES-NI, SHA256, and RSA/ECC enhancements along with SecureKey support.

BMI optimizations improve both speed and performance, so instead of just running the hash functions in software, they can take better advantage of Intel® architecture cryptography, which in turn greatly improves the performance of their algorithms. Thompson said this is an example of wolfSSL's commitment to continual improvement, which she sees as a crucial reason for their recurring presence.

In a recent press release, Larry Stefonic, CEO of wolfSSL, agreed. “Handcrafting the world’s best crypto is our nature,” he said, “so it is great to leverage Intel’s fantastic engineering support for the primitives to enhance our product. Our wolfSSL customers will enjoy better performance as a result of these software optimizations on 5th generation Intel Core processors.”

Details on performance can be found in the wolfSSL blog.

Download the latest release of wolfSSL.

Learn more about Intel® Secure Key Technology.