Development and Benchmarking of Cryptographic Implementations on Embedded Platforms

Master's Thesis Defense
by
John Pham
Committee Members
Dr. Jens-Peter Kaps (Director)
Dr. Kris Gaj
Dr. Craig Lorie
Friday, July 31, 2015, 11:00AM
ENGR 4801

Abstract

In 2007, the National Institute of Standards and Technology (NIST) announced the Secure Hash Function-3 (SHA-3) competition to select a successor of the SHA-2 standard after vulnerabilities were discovered in the related SHA-1 algorithm. The Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) was announced in 2013 to select algorithms for Authenticated Encryption and Associated Data (AEAD) that exceeded the performance of Advanced Encryption Standard-Galois Counter Mode (AES-GCM). As part of both competitions, algorithm implementations in hardware and software were compared in order to evaluate the performance and other characteristics. An area of interest is performance on embedded devices, where resources are more constrained.

Embedded devices are becoming increasingly interconnected. Formerly "dumb" appliances, such as thermostats, light bulbs, door locks, coffeemakers, and insulin pumps now have the ability to connect to the Internet. This is done in order to allow remote control and monitoring. Therefore, their communications need to be secured via encryption, in order to maintain privacy, or prevent malicious control. This may come at the cost of increased complexity, decreased throughput, increased energy consumption, and increased storage or die area.

In this thesis, we describe our support of the SHA-3 and CAESAR competitions. We made a lightweight implementation of the SHA-3 finalist JH in hardware on FPGAs as part of a comparison between other lightweight implementations of SHA-3 finalists. For fair, comprehensive, and automated evaluation of hardware, the Computer Engineering Research Group (CERG) at George Mason University (GMU) developed the ATHENa tool. We supported this effort by creating a searchable online database to store and present the results to the research community. For software, the eXternal Benchmarking eXtension (XBX) evaluates SHA-3 candidates on several microcontrollers. We ported XBX to the MSP430 platform and reported results.

As part of the CAESAR competition, we overhauled XBX to cover Authenticated Encryption and Associated Data (AEAD) ciphers, ported the test harness to a more capable platform, and proposed a means to measure power. We also extended the ATHENa database to support authenticated ciphers.