ITL BULLETIN FOR JUNE 2017

TOWARD STANDARDIZING LIGHTWEIGHT CRYPTOGRAPHY

Kerry A. McKay, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

The world is increasingly interconnected by myriads of devices, working in concert to accomplish important tasks, including automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. But these devices may have resource restrictions, compared to common desktop computers. For example, they may have significantly reduced power consumption, less computation power, and orders of magnitude less memory than desktop computers. These constraints can make it difficult to implement modern cryptographic algorithms, most of which are designed for desktop or server environments. To address this issue, different cryptographic algorithms have been tailored for resource-constrained devices. The academic community has performed a significant amount of work on this type of cryptography, called lightweight cryptography. This work includes efficient implementations of conventional cryptography standards and the design and analysis of new lightweight algorithms and protocols.

In 2013, NIST's Information Technology Laboratory started a lightweight cryptography project to investigate the issues and then develop a strategy for the standardization of lightweight cryptographic algorithms. In 2015 and 2016, NIST held two lightweight cryptography workshops to solicit public feedback on the constraints and limitations of the target devices, and the requirements and characteristics of real-world applications of lightweight cryptography.

Recently, NIST decided to create, through an open process, a portfolio of lightweight algorithms. ITL has published NIST Internal Report (NISTIR) 8114, *Report on Lightweight Cryptography*, to summarize the findings of this project and to outline NIST's plans for the standardization of lightweight algorithms. Here, we present highlights from this report, especially the devices targeted by lightweight cryptography, how the algorithms were designed, and the standardization of lightweight cryptographic algorithms.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

Devices Targeted by Lightweight Cryptography

Lightweight cryptography targets a wide variety of devices that can be implemented on a broad spectrum of hardware and software. On the high end of the device spectrum are servers and desktop computers followed by tablets and smartphones. Conventional cryptographic algorithms generally perform well in these devices; therefore, these platforms do not require lightweight algorithms. The lower end of the device spectrum contains more constrained devices, such as embedded systems, Radio-Frequency IDentification (RFID) devices, and sensor networks. Lightweight cryptography is primarily focused on the highly constrained devices that can be found at this end of the spectrum.

Lightweight algorithms may be subject to various constraints, such as performance requirements, stringent timing, and power requirements, which will be explored during the first phase of the standardization effort.

While lightweight cryptography primarily targets devices at the low end of the device spectrum, it is important to note that it may be necessary to implement lightweight algorithms at the high end of the spectrum as well. For example, many resource-constrained sensors may send information to an aggregator (e.g., a server) that, by most accounts, is not constrained. However, the aggregator must support lightweight algorithms to interoperate with the constrained sensors when they use lightweight cryptographic algorithms. In short, the environment and application need to be factored into the decision of whether conventional standards are acceptable. It is not just the limitation of a device that drives the need for lightweight cryptography, but also the other devices in the application with which it directly interacts.

Design of Lightweight Algorithms

In cryptographic algorithm design, a trade-off between performance and resources is required for a given security level. Performance can be expressed in terms such as power and energy consumption, latency, and throughput. The resources required for hardware implementation are usually summarized in gate area, gate equivalents, or logic blocks (also known as configurable logic blocks, logic elements, adaptive logic modules or slices). In software, this trade-off is reflected in register, random-access memory (RAM), and read-only memory (ROM) usage. Resource requirements are sometimes referred to as costs, as adding more gates or memory tends to increase the production cost of a device.

Over the past decade, many lightweight cryptographic primitives – including block ciphers, hash functions, message authentication codes, and stream ciphers – have been proposed, which offer performance advantages over conventional cryptographic standards. Unlike conventional algorithms, lightweight primitives are not intended for a wide range of applications and may impose limits on the power of the attacker. For example, the amount of data available to the attacker under a single key may be limited.

But these limitations do not mean that the lightweight algorithms are weak. Rather, they are designed to achieve an effective balance among security, performance, and resource requirements for specific resource-constrained environments. NISTIR 8114 provides the results of analysis and comparison of lightweight cryptographic primitives and conventional cryptographic standards, emphasizing the benefits of the former for certain applications.

The report also discusses the performance of NIST-approved cryptographic standards – such as block ciphers, hash functions, authentication encryption algorithms, and stand-alone message authentication codes (MACs) – in resource-constrained environments, and it provides some recommendations for use of those standards.

Lightweight Cryptography Standardization

NIST develops cryptographic standards using several different approaches, such as competitions that NIST convened to select the AES (Advanced Encryption Standard) block cipher and the SHA-3 hash functions. These competitions were significant efforts that took place over many years. For example, the SHA-3 competition began in 2007, the winner was announced in 2012, and the standardization process was concluded in 2015.

Another approach is to adapt standards of other accredited standards development organizations, as was done with keyed-hash message authentication code (HMAC) and RSA standards. NIST researchers also develop standards and guidelines in collaboration with experts in academia, industry, and government, if no suitable standard exists.

The landscape for lightweight cryptography is moving so quickly that a standard produced using the competition model is likely to be outdated prior to standardization. Therefore, the most suitable approach for lightweight cryptography, in terms of timeline and project goals, is to develop new recommendations using an open call for proposals for existing algorithms that could be standardized.

NIST plans to develop and maintain a portfolio of lightweight algorithms and modes that are approved for limited use within the U.S. federal government. Each algorithm in the portfolio will be tied to one or more *profiles*, which consist of algorithm goals and acceptable ranges for metrics. This contrasts with other primitives and modes that are approved for general use.

Profiles will be designed to target classes of devices and applications – not necessarily specific applications. Profiles will be useful across a variety of applications. NISTIR 8114 provides the characteristics that have been identified to be addressed in profiles. The appropriateness of an algorithm depends on the physical limitations of the device and the performance and security objectives imposed by the application.

To build relevant profiles for a variety of applications, NIST asks a series of questions to the stakeholders of lightweight cryptography. NISTIR 8114 lists the questions, proposes a template for profiles, and provides some possible next steps for the ongoing NIST activities related to lightweight cryptography.

Summary

NISTIR 8114 provides an overview of lightweight cryptography and outlines NIST's plans regarding development of a portfolio of lightweight algorithms. The report presents to stakeholders of lightweight cryptography a series of questions that will help build relevant profiles for a variety of applications. Based on community discussion and responses to the questions, NIST will develop profiles about application and device requirements for lightweight cryptography. Algorithms will be recommended for use only in the context of profiles, which describe physical, performance, and security characteristics.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.