

Profile Development

Lightweight Cryptography Workshop 2016

October 17, 2016

Kerry McKay, NIST

What is a Profile?

- A profile summarizes requirements for class of devices and applications
 - Physical, performance, and security characteristics
 - Design goals

Physical characteristics	Performance characteristics	Security characteristics
Area (in GE)	Latency (in clock cycles)	Minimum security strength (bits)
Memory (RAM/ROM)	Throughput (cycles per byte)	Attack models
Implementation type (hardware, software, or both)	Power (μ W)	Side channel resistance requirements

Why Profiles?

- It would certainly be easier to have general recommendations
 - Approach taken with most NIST standards and guidelines
- Unlike current NIST primitives, we don't expect the portfolio to be composed of only general-use algorithms
- Performance gains may be achieved by eliminating properties that are not needed for a particular application

Why Profiles? (continued)

- Algorithms will only be recommended in context of profiles
 - Application and device requirements matched to algorithm properties
 - I.e., algorithms for profile X will not be NIST-recommended for application Y if the requirements do not match those of profile X
- Algorithms cannot be recommended in cases where necessary properties are not present
 - E.g., can't recommend hash function with low collision resistance for application that requires high collision resistance

What Will a Profile Look Like?

- Proposed a template in draft NISTIR 8114
- Draft contained template and examples

Profile <profile name>	
Primitive	<i>Type of primitive</i>
Physical characteristics	<i>Name physical characteristic(s), and provide acceptable range(s) (e.g., 64 to 128 bytes of RAM)</i>
Performance characteristics	<i>Name performance characteristic(s), and provide acceptable range(s) (e.g., latency of no more than 5 ns)</i>
Security characteristics	<i>Minimum security strength, relevant attack models, side channel resistance requirements, etc.</i>
Design goals	<i>List design goals.</i>

Sample 1

- MAC for RFID asset tracking
 - Low-area
 - Small amounts of data

Profile Sample_1	
Primitive	MAC
Physical characteristics	1600 to 1900 GEs, ASIC hardware implementation
Performance characteristics	Latency \leq 15 ns
Security characteristics	128-bit security, resistance to related key attacks, timing analysis
Design goals	Efficient for short input messages

Sample 2

- Block cipher that may be appropriate for command validation on Controller Area Network (CAN) bus

Profile Sample_2	
Primitive	Block cipher
Physical characteristics	Hardware or software implementation
Performance characteristics	Latency ≤ 20 ns
Security characteristics	128-bit security, resistance to power analysis
Design goals	Authenticated encryption

Sample 3

- MAC that may be appropriate for a sensor network node
- Same MAC algorithm could be recommended for both sample 1 and sample 3

Profile Sample_3	
Primitive	MAC
Physical characteristics	Hardware implementation
Performance characteristics	Power $\leq 10 \mu\text{W}$
Security characteristics	128-bit security, resistance against related key attacks, power analysis
Design goals	Resistance against tag forgeries

Questionnaire

- We've received interest and support for this project
 - Received feedback after 2015 workshop and in discussion with interested parties
- What we are missing is specific information needed to make profiles
 - Information specific to applications, devices, and operating environments
- Questionnaire intended to learn what the requirements for application and its devices are
 - We will consider all input we receive outside the questionnaire as well

Questionnaire Responses

- We asked for response by October 1 in order to develop profiles to discuss here
 - We are still listening – keep sending them in if you have a use case for lightweight crypto algorithms where you'd like a NIST standard
- By Oct 1, there were two responses to the questionnaire
 - One for RAIN RFID anti-counterfeiting applications
 - One that attempted to answer the questions for many applications using specific processors

From Responses to Profiles

- The main idea is to group similar use case requirements together into profiles
- We had hoped to receive enough feedback to present initial profiles here
 - Only had one use case we could create a profile for

Profile Development

- Call for profile information is continuous
- Draft profiles will be posted with 30 day comment period
 - Posted on computer security resource center
 - <http://csrc.nist.gov>
 - Announced on lwc-forum mailing list
- Calls for algorithms will come after a profile is finalized
 - Profile gives the algorithm requirements

How Many Profiles?

- Short answer: we don't know
 - This will be driven by community needs and ability to group similar requirements into single profile
- Don't expect a one-to-one mapping of use cases to profiles, or algorithms to profiles
 - Several use cases could have similar requirements, leading to a single profile that serves them all
 - One algorithm may be recommended for multiple profiles
- Don't want more profiles than we think we need

How Many Profiles? (continued)

- Bigger concern: number of recommended algorithms
 - Too many becomes a maintenance issue for developers (and us)
 - Keep number of algorithms in portfolio as low as possible

Other Applications

- In conversation, interest in other applications have been expressed, such as
 - CAN bus
 - Connected soldier
 - CubeSats
 - Smart manufacturing
- Need to follow up and seek more input from community

Questions

- Is there anything missing from the questionnaire?
- In profiles, should performance characteristics be hard or soft?
 - E.g., “low-latency” vs. “latency < X”
- How specific should profiles be?
- What more could/should we add to profiles?
- Is a 30-day public comment period long enough to review draft profiles?
- How much information about the use cases does NIST need to provide reviewers in order to evaluate the profiles during the public comment period?
- Are there any barriers to sharing profile requirements, such as intellectual property concerns?
 - Can we make the questionnaire responses public?