Lightweight Cryptography for Resource-Constrained Devices

Andrea Visconti

Computer Science Department "Giovanni degli Antoni"
University of Milan

http://www.di.unimi.it/visconti

andrea.visconti@unimi.it

Overview

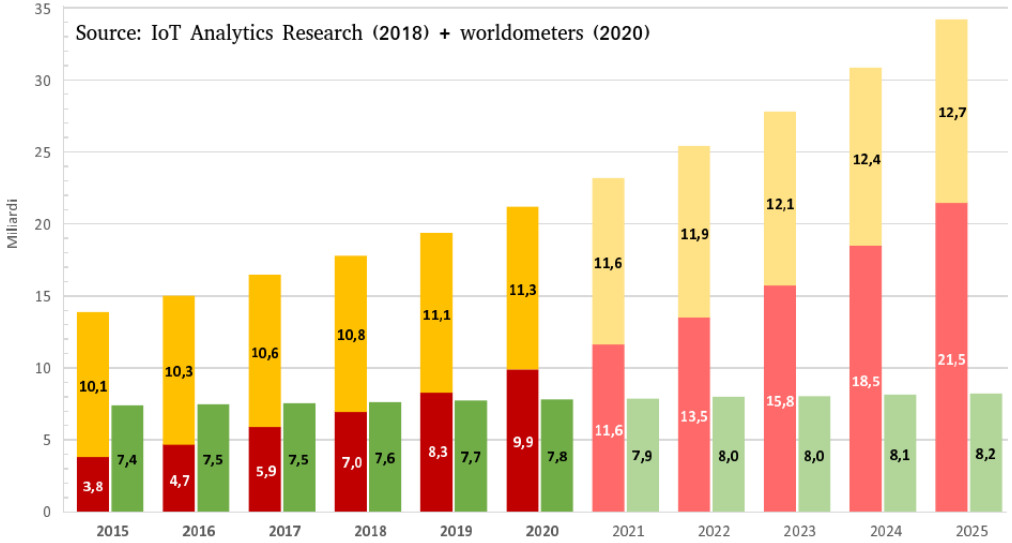
1. Introduction and problem description;
2. Cryto for IoT Devices and state of art;
3. Concluding remarks.

Introduction and problem description

Milestones:

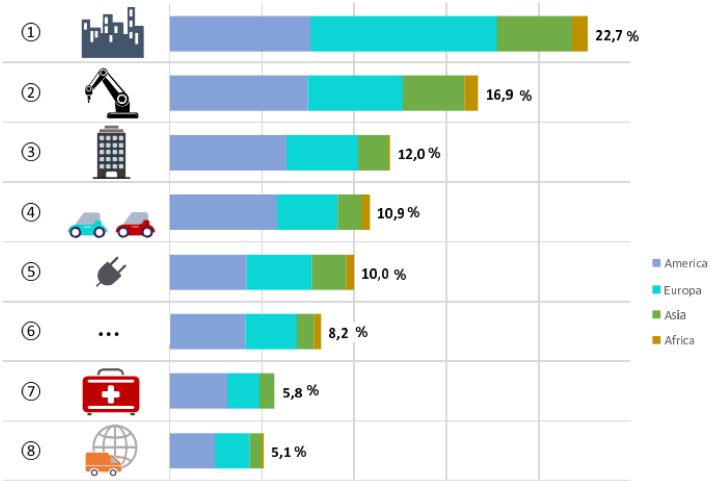
- 1982: Carnegie Mellon University
- 1999: IoT and RFID
- 2000: LG Electronics
- ...
- 2008: IoT conference
- 2009: Fully-self driving cars
- 2009: IoT and healthcare
- ...

Introduction and problem description



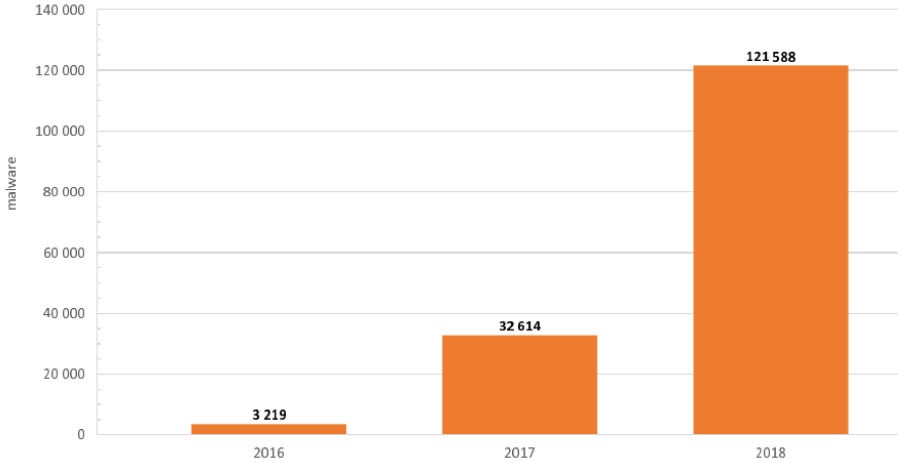
Introduction and problem description

Source: IoT Analytics (Jan 2018)



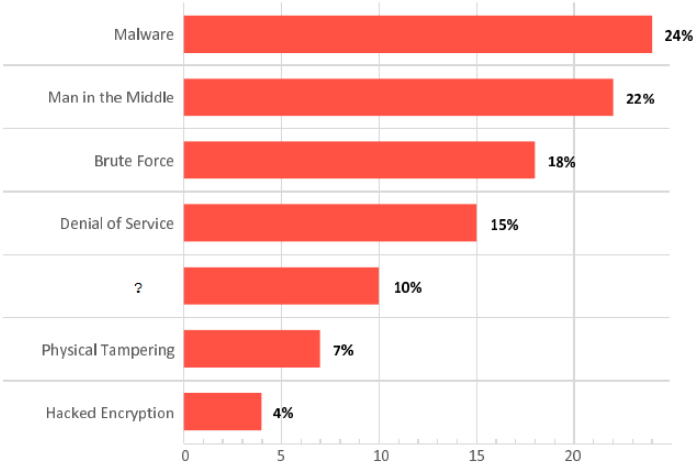
Introduction and problem description

Kaspersky Lab: New IoT-malware grew three-fold in H1 2018



Introduction and problem description

The most common attacks (2015-2017) on IoT devices are:



Introduction and problem description

Cyber attacks... why?

Most often, cyber attacks happen because users **have not** (or **have incorrectly**) implemented cryptographic techniques:

- **Users avoid crypto**... crypto means low performance, crypto means power consumption;
- **Adoption of weak cryptographic functions** (e.g. DES, TEA) — Brute-force attack;
- **Adoption of deprecated cipher suite** in SSL/TLS protocol (e.g. weak RSA keys, MD5, downgrade attack) — Man-in-the-middle attack;
- ...

Lightweight

We have to define the **weight of an algorithm**. The weight of a primitive is the **amount of resources necessary to run the primitive itself**...

- in time;
- in space;
- in software;
- in hardware;

Introduction and problem description

... in software

- the number of clock cycles necessary to execute one byte of data (**speed**);
- the number of clock cycles of overhead (**latency**);
- the amount of RAM necessary to carry the computation (**memory complexity**);
- the space required to store the algorithm — e.g. in a flash memory.

Introduction and problem description

... in hardware

- the amount of data processed in one second using a given clock frequency, for example 100Hz (**time efficiency** or **throughput**);
- the time which must be taken, for example, to derive the sub-keys before they can be used (**latency**);
- the number of gates necessary to implement a primitive (**GE**[a]**, Gate Equivalence**) — e.g. $<$ 2000 GE;
- a low **average** power consumption (**power consumption**) — e.g. $<$ 1-10 μW/MHz;
- a reasonable **peak** power consumption (**power consumption**) — e.g. $<$ 3-30 μW/MHz;

[a] 1 GE = 1 NAND gate.

Introduction and problem description

Notice that

- lightweightness in hardware doesn't imply lightweightness in software;
- lightweightness software in doesn't imply lightweightness in hardware.

Primitives:

- lightweight block ciphers
- lightweight hash functions
- lightweight stream ciphers
- ...

We are talking about pre-NIST "competition".

Cryto for IoT Devices and state of art

There is a long list of lightweight **block ciphers** (cryptoLUX):

3 Substitution-Permutation Network
- 3.1 AES-like
  - 3.1.1 AES
  - 3.1.2 KLEIN
  - 3.1.3 LED
  - 3.1.4 Midori
  - 3.1.5 Mysterion
  - 3.1.6 SKINNY
  - 3.1.7 Zorro
- 3.2 Bit-SIiced S-Boxes
  - 3.2.1 Fantomas/Robin
  - 3.2.2 Noekeon
  - 3.2.3 PRIDE
  - 3.2.4 Rectangle
- 3.3 Other SPN-based Structures
  - 3.3.1 mCrypton
  - 3.3.2 MANTIS
  - 3.3.3 PRESENT
  - 3.3.4 PRINCE
- 3.4 ARX-Based SPN
  - 3.4.1 SPARX

4.1 ARX-Based
- 4.1.1 Chaskey Cipher
- 4.1.2 HIGHT
- 4.1.3 LEA
- 4.1.4 RC5
- 4.1.5 SIMECK
- 4.1.6 SIMON and SPECK
  - 4.1.6.1 SIMON
  - 4.1.6.2 SPECK
- 4.1.7 XTEA

4.2 Two Branched
- 4.2.1 DESLX
- 4.2.2 GOST revisited
- 4.2.3 ITUbee
- 4.2.4 KASUMI/MISTY
  - 4.2.4.1 MISTY
  - 4.2.4.2 KASUMI
- 4.2.5 LBlock
- 4.2.6 RoadRunneR
- 4.2.7 SEA

4.3 Generalized Feistel Networks (GFN)
- 4.3.1 CLEFIA
- 4.3.2 Piccolo
- 4.3.3 TWINE

5 Other Designs
- 5.1 KTANTAN and KATAN

Cryto for IoT Devices and state of art

There is a long list of lightweight **hash functions** (cryptoLUX):

Cryto for IoT Devices and state of art

There is a long list of lightweight **stream ciphers** (cryptoLUX):

3 Descriptions
- 3.1 A5/1
- 3.2 ChaCha
- 3.3 E0
- 3.4 FCSR-based Stream-Ciphers
  - 3.4.1 F-FCSR-H v3
  - 3.4.2 F-FCSR-16 v3
- 3.5 Grain
- 3.6 MICKEY v2
- 3.7 SNOW 3G
- 3.8 Trivium

Unfortunately there isn't an international standard... not yet!

Cryto for IoT Devices and state of art

Open-source Libraries (Casati, M.Sc Thesis, 2020):

	mbed TLS	wolfSSL	LibTomCrypt	AVR-Crypto-Lib	Wiselib	TinyCrypt	A. C. L.	TinyECC	L. C. L.	RELIC
Block Ciphers	7	5	22	18	1	1	2	0	3	1
Stream Ciphers	2	3	6	7	0	0	1	0	0	0
Asymmetric	5	6	6	4	4	3	4	4	0	4
Hash Functions	6	8	10	13	1	1	4	1	0	3
Documentation										

Cryto for IoT Devices and state of art

Ciphers implemented:

- **Symmetric** (Block Ciphers): 3DES, AES, Blowfish, Camellia, Kasumi, IDEA, Cast, Piccolo, RC5, RC6, Aria, Seed, XTEA, Speck, Present, ...
- **Symmetric** (Stream Ciphers): RC4, Chacha, Salsa20, Grain, Sosemanuk, Trivium, ...
- **Asymmetric**: DH, ECDH, DSA, ECDSA, RSA, ...
- **Hash Functions**: SHA1, SHA2, SHA3, MD2, MD4, MD5, BLAKE, RIPEMD, WHIRLPOOL, ...

Cryto for IoT Devices and state of art

Lightweight Cryptography for IoT Devices

NIST has initiated a process to evaluate and **standardize lightweight crypto algorithms** for IoT Devices.

Why?

Because current cryptographic standards (that we use every day) were designed for **desktop environments** (or server environments).

These algorithms usually **don't fit** into IoT devices — e.g. AES about 1500 GE (encryption only!! no decryption, no key schedule), the internal state of SHA-3 requires 1600 bits, SHA-2 requires 512 bits, etc.

Cryto for IoT Devices and state of art

NIST-approved crypto standards

- FIPS 197 (AES) + FIPS 800 38 series (Modes of Operation)
- FIPS 180 (SHA-1 SHA-2) + FIPS 202 (SHA-3)
- GMAC, CMAC, HMAC, KMAC
- Signatures, Key-derivation, ...

Examples of constrained devices:

- RFID tags;
- Sensor networks;
- IoT devices.

Cryto for IoT Devices and state of art

Some applications

- RFID anti-counterfeiting (using challenge-response protocols);
  - RFID chips have a small amount of memory;
- Driving assistance system (in-vehicle, vehicle-to-vehicle, road-to-vehicle communication);
  - High throughput, low latency;
- Medical sensor (measuring blood pressure, blood sugar, etc.)
- Smart home appliances;
- ...

Cryto for IoT Devices and state of art

LWC initiatives

eSTREAM (2004-08), CRYPTREC, CEASAR (2014-18), ISO/EIC.

- LWC ciphers have to operate as authenticated encryption/decryption algorithms
- AE **avoids chosen ciphertext attacks** that take advantage against a cryptosystem by submitting carefully chosen ciphertexts and analyzing the decrypted results;
- AEAD **avoids to cut-and-paste a valid ciphertext** into a different context;
- LWC ciphers may operate as hash functions;
- LWC ciphers have to define unambiguously padding rules, IVs, Authenticated Associated Data;
- LWC ciphers have to provide **theoretical** and **empirical evidence** for security claims.

Cryto for IoT Devices and state of art

NIST published a call for algorithms (**August 2018**) and it received about 60 submissions (**February 2019**).

During the Round 1, several candidates were eliminated from consideration (**Feb-Aug 2019**) — forgery attacks, distinguishing attacks, undesirable properties, . . . ;

NIST selected the Round 2 candidates: 32 algorithms (**August 2019**)

The Round 2 candidates update on their algorithms — new security profs, new SW and HW implementations, new third-party analysis, etc. (**Aug 2019 - March 2021**).

NIST annunced the Lightweight Cryptography finalists (**March 2021**).

Cryto for IoT Devices and state of art

The finalists are

ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodyak.

Last round of the NIST LWC Standardization Process

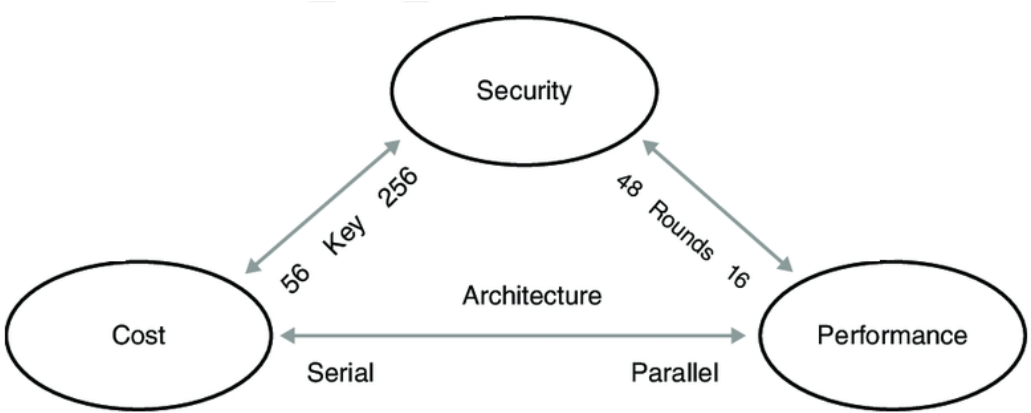
- Finalists provided updated submission packages;
- Minor modifications, no larger modifications;
- Same submission requirements of the original call for algorithms;
- This round is expected to last about 1 year.

Cryto for IoT Devices and state of art

The main characteristics of LWC Crypto Algorithms are:

- 4x4 SBoxes (instead of 8x8),
- bit permutations,
- many iteration of simpler rounds,
- simpler key schedules.

Cryto for IoT Devices and state of art



Concluding remarks

Optimizations...

- HW and SW optimizations;
- Speed and latency;
- Optimizing Primitives;

Security...

- Linear and Differential Cryptanalysis;
- SW Implementations (bugs, flaws, unexpected behaviors, ...);
- HW Implementations (Side-channel attacks, fault attacks, ...).

Tradeoff between...

- Security VS Cost VS Performace.

Thanks for your attention!

http://www.di.unimi.it/visconti