HITACHI
Inspire the Next

On the standardization of cryptographic application techniques for IoT devices in ITU-T and ISO/IEC JTC 1

November 5, 2015

Hirotaka Yoshida, Ph.D.
Security Research Dept.
Center for Technology Innovation-Systems Engineering
Hitachi, Ltd., Research & Development Group

HITACHI
Inspire the Next

Contents

1. Background
2. The status of standardization in ITU-T
3. The status of standardization in ISO/IEC JTC1
4. Summary

HITACHI
Inspire the Next

Contents

1. Background
2. The status of standardization in ITU-T
3. The status of standardization in ISO/IEC JTC1
4. Summary

HITACHI
Inspire the Next

Contents

1-1 IoT security activities in standardization organizations

HITACHI
Inspire the Next

IoT(Internet of Things): System producing a new value by sensing and analyzing "Thing" connected to the network

- Many standardization organizations start IoT security study since 2004

Standardization organizations	Field	Target	Objective
ETSI TC ITS WG5	Antenna	ITS communication devices in Vehicles	ITS platform/foundations/users protection
3GPP SA3	Antenna	Smart phones	Security and privacy in 3GPP*1systems
oneM2M WG4	HEMS/Antenna	Smart meters, TV, hot water heater, vehicles	M2M-service-common-platform security
IETF LoWPAN	WirelessAP/router/ HEMS	Production equipments, air conditioner, Smart meters,	Light overhead protocol in 6LowPAN*2protcol security
IEEE P2413 WG	Wireless AP/HEMS/ Antenna	Air conditioner, hot water heater, Vehicles	IT systems, vehicle systems, IoT application framework (that abstracts plants) security
ISO/IEC JTC1/ SC 27	Wireless AP/router/ HEMS/Antenna	Production equipments, air conditioner, Smart meters, hot water heater, vehicles, surveillance cameras, smart phones	Standard of low resource cryptographic primitives for IoT devices
ITU-T SG17	Wireless AP/router HEMS/Antenna	Production equipments, air conditioner, smart meters, hot water heater, vehicles, surveillance cameras, smart phones	Security of communication between IoT devices

【Observation】Trains are not covered as standardizing target because it might has been studied in a closed manner

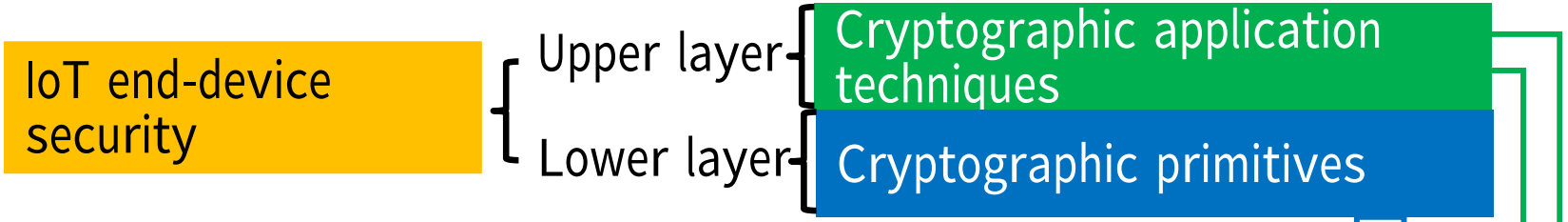
- Focus in this presentation
  - ✓ Explain standardization that goes from devices at lower layer to the upper application layer
  - ✓ IoT related projects in ITU-T SG17 and ISO/IEC SC27

*1: The third generation mobile phone(3G)systems, The 3.9 generation mobile communication systems, LTE, standardization project for the 4th generation mobile communication systems, LTE-Advanced
*2: Low power mesh network where each node with dedicated IPv6 address can directly connect to the internet using open standard

HITACHI
Inspire the Next

This presentation focuses IoT end-device security

- IoT end-device security is realized by counter measures at the two layers



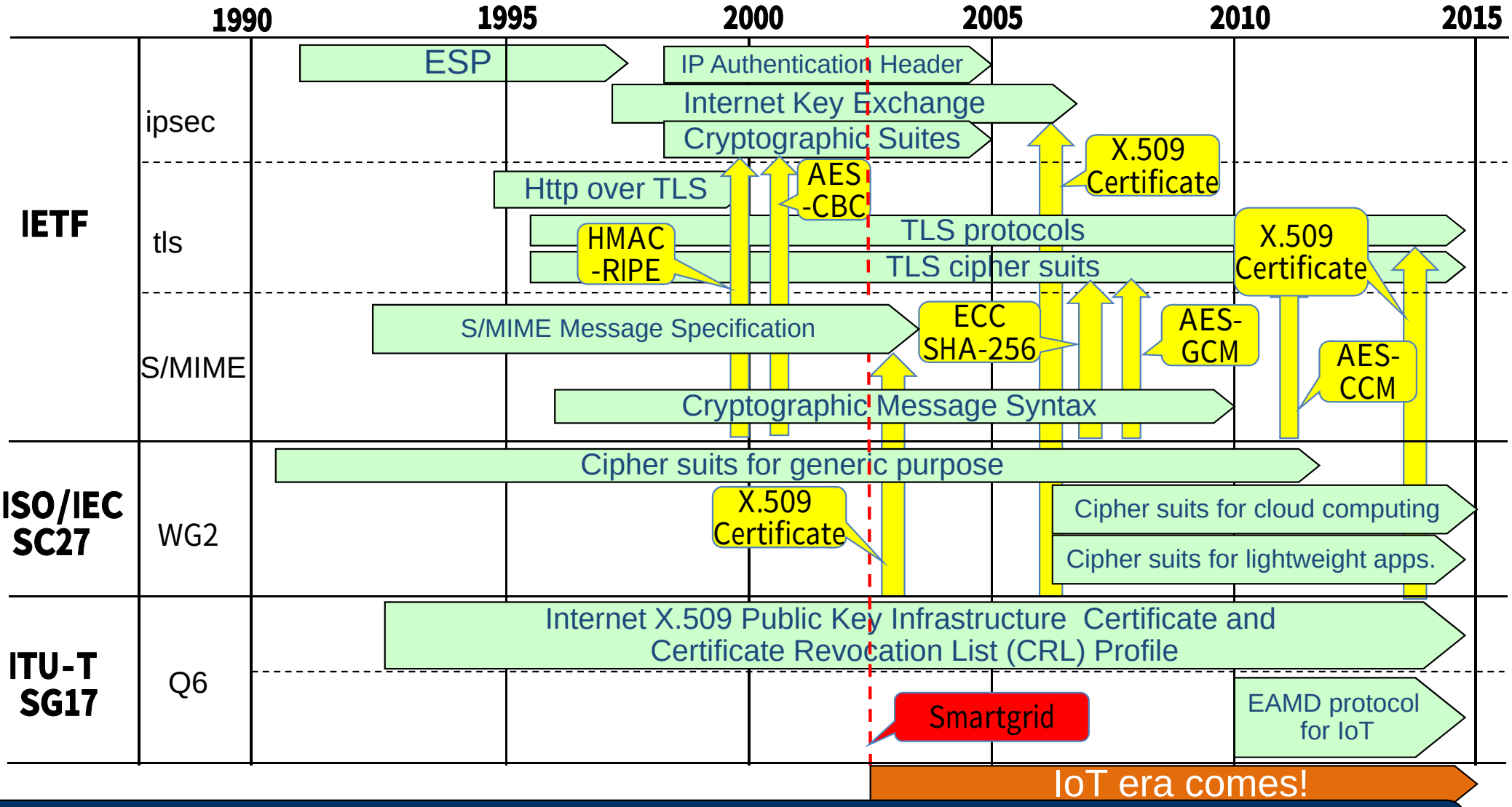
- Standardization organizations regarding IoT security
  - ETSI TC ITS WG2
  - GSMA
  - IEEE P2413 WG
  - IETF LoWPAN
  - ISO/IEC JTC 1/SC 27
    - ✓ lightweight cryptgraphy standardizationproject: 29192*1
  - ITU-T SG17
    - ✓ IoT end-device security standardizationproject: X.iotsec
  - oneM2M WG4
  - 3GPP SA3

This presentation explains standardization in ITU-T and ISO/IEC

1-3 IETF/ISO/ITU-T historical background

HITACHI
Inspire the Next

IETF is highly appreciated for having developed security protocols such as Ipsec, TLS, and S/MIME.
ITU-T and ISO/IEC quietly delivers security fundamentals such as cipher suits and X.509 certificate.



Hereafter, this presentation provides potentially-bridge information to consider:

"What could be collaboration between IETF for de-facto and ISO/ITU-T for de-jour in IoT era?"

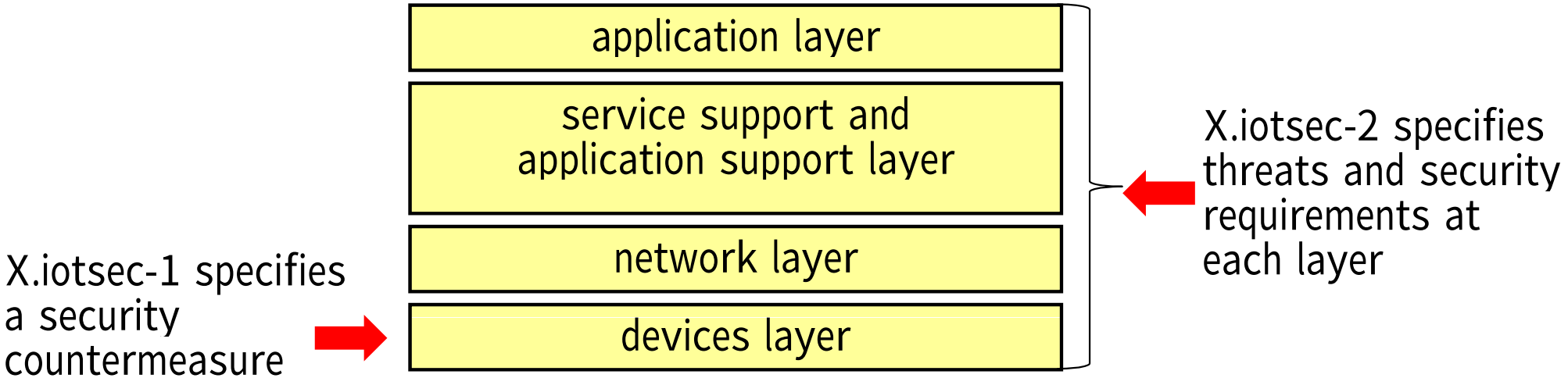
HITACHI
Inspire the Next

Contents

2 - 1 IoT security study in ITU - T SG17

HITACHI
Inspire the Next

- ITU-T SG17
  - ✓ Standardization organization regarding telecommunication security (Discussions since in 2001)
  - ✓ Consists of 5 WPs
    - ➢ Foundation security (WP1), network・information security (WP2), ID management and cloud computing security (WP3), application security (WP4), formal language (WP5)
- The status of IoT related projects
  - ✓ Study in ITU-T SG17 WP4
  - ✓ In the ITU-T IoT reference model, IoT related project specifies the following
    - ➢ X.iotsec-1：specify a security countermeasure at the device layer
    - ➢ X.iotsec-2：specify threats and security requirements at each layer



IoT reference model

2 - 2 X.iotsec - 1 abstract

HITACHI
Inspire the Next

- Scope
  - ✓ It provides encryption procedure that achieves realtime requirement and low resource requirements for security communication between IoT devices
- Editor
  - ✓ Japan(Hitachi., Ltd)
- Main standardization contents
  - ✓ Specification of how to communicate cryptographic application mechanism EAMD[*1] (communication flow, packet format)
  - ✓ Specification of the abstract of EAMD specification(basic data flow, parameter set)
  - ✓ Specification of how to communicate using cryptographic primitives such as AES-GCM etc. and packet authentication is possible.
  - ✓ Guideline on how to use cryptographic parameter

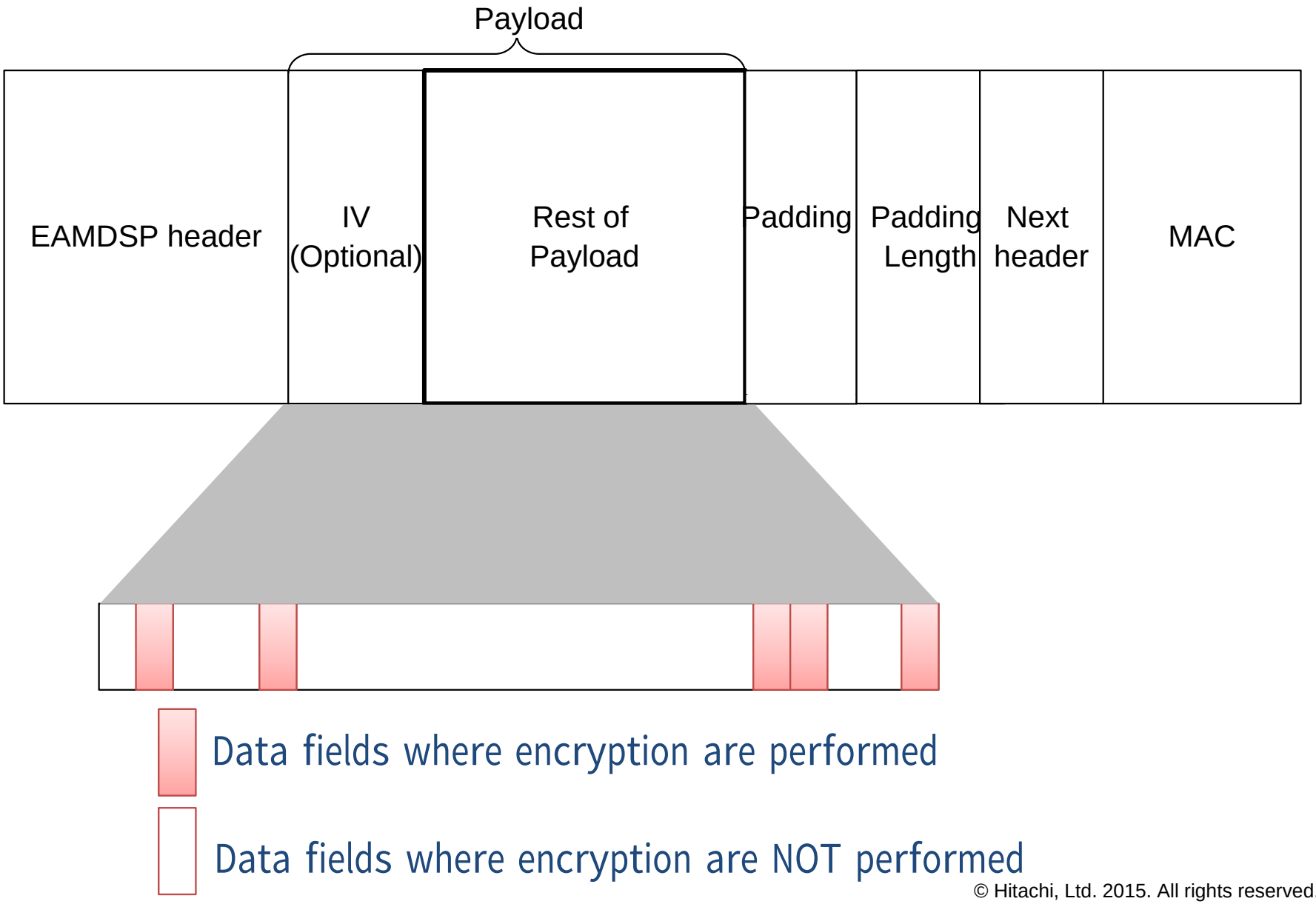
Hitachi's activity: standardization of Hitachi-developed cryptographic application mechanism: EAMD

*1 encryption with associated mask data

2 - 3 Packet format in EAMD-used communication

HITACHI
Inspire the Next

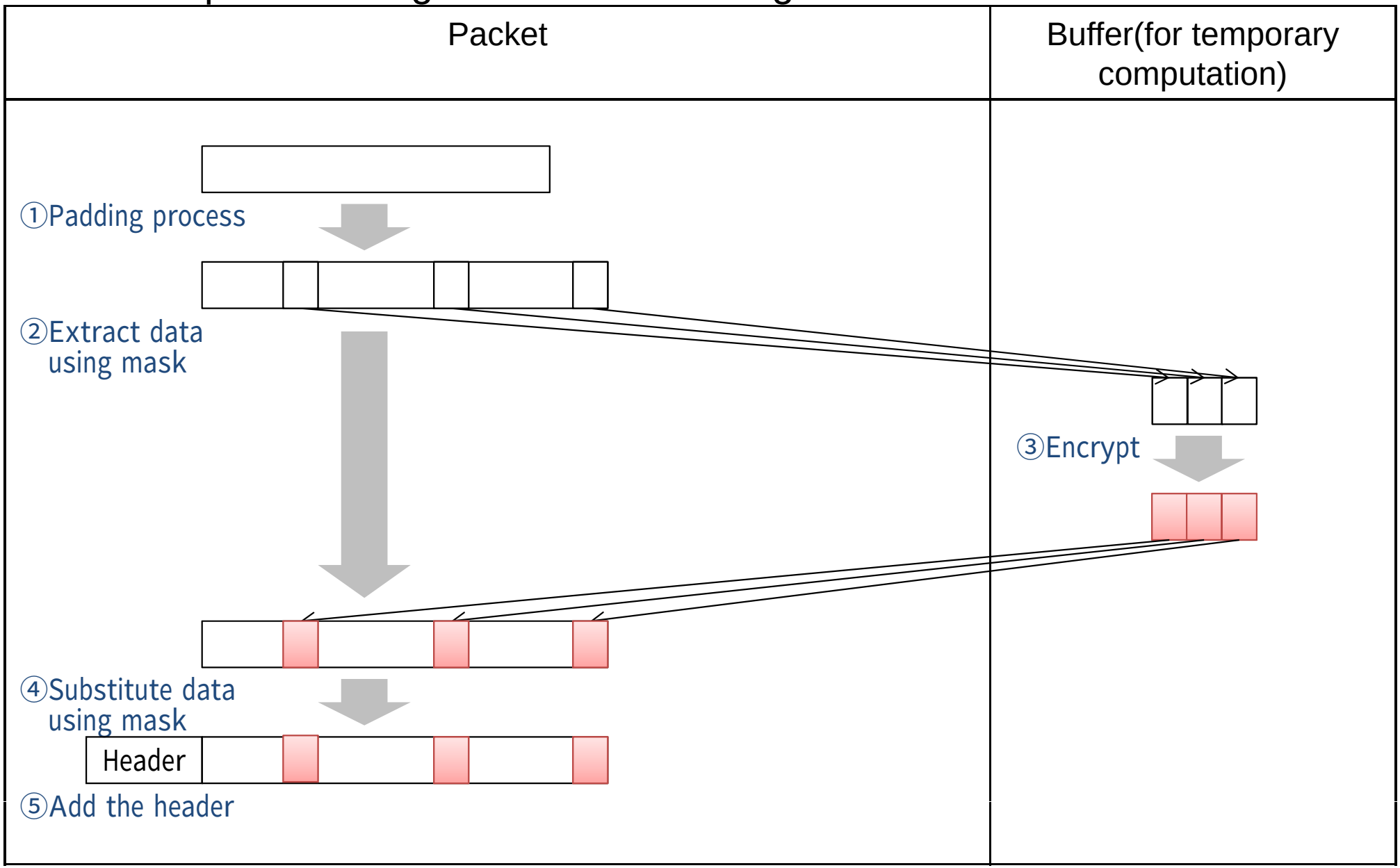
- Reduce the overhead by encrypting the only data that are sensitive



2 - 4 Packet sending flow in EAMD-used communication

HITACHI
Inspire the Next

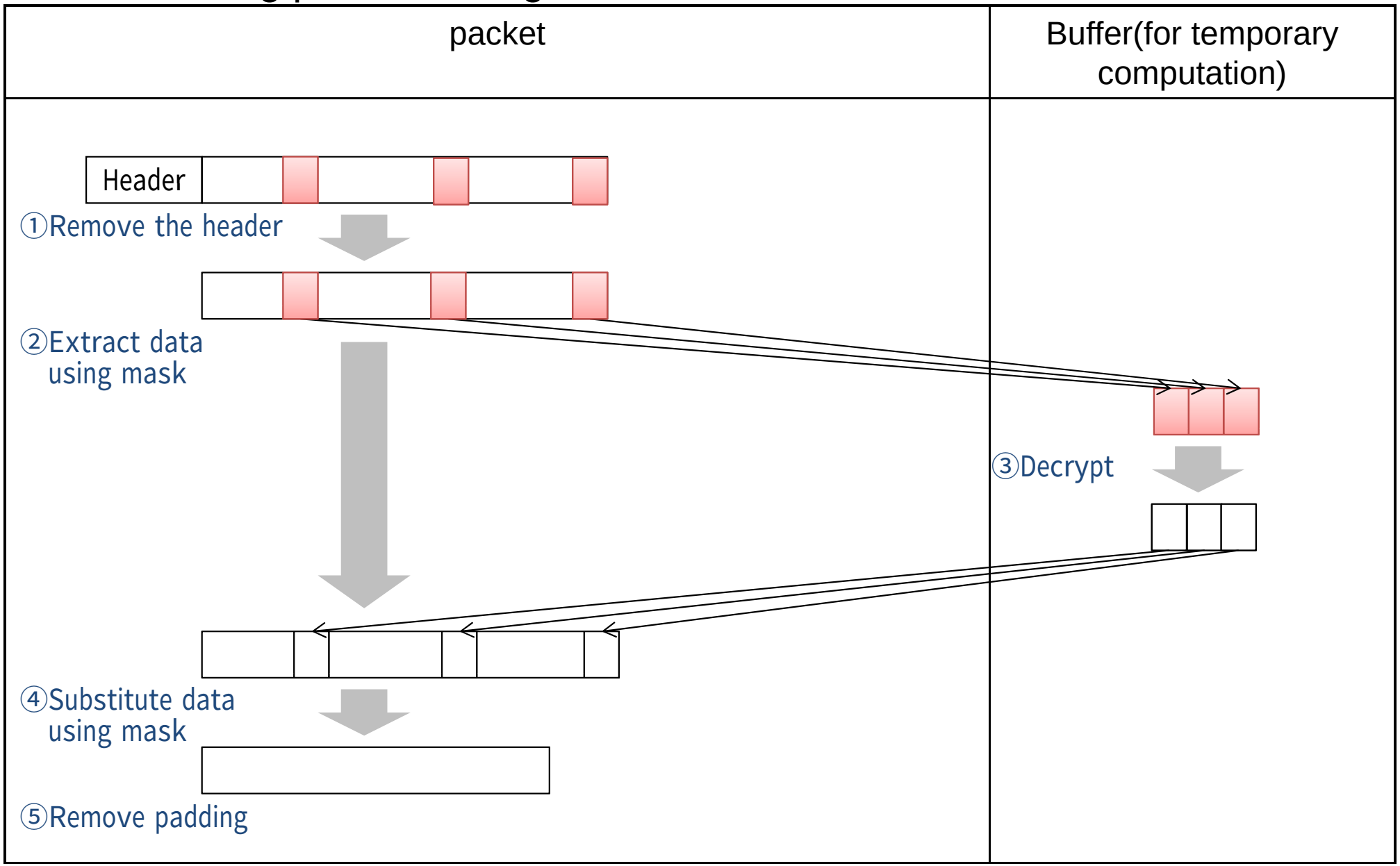
- Generate packet using the mask indicating sensitive data location



2 - 5 Packet receiving flow in EAMD-used communication

HITACHI
Inspire the Next

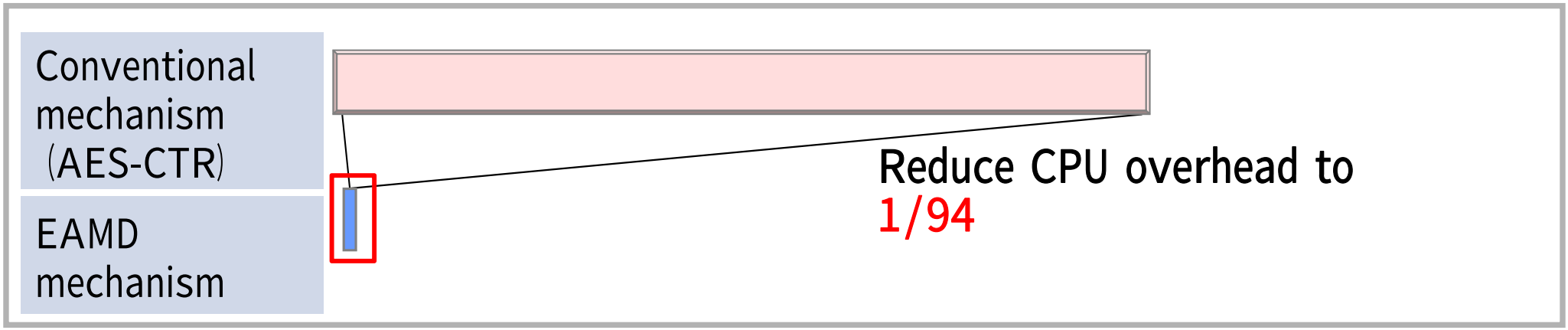
- Packet storing process using the mask that has been shared in advance



2 - 6 Impact of EAMD

HITACHI
Inspire the Next

- Performance comparison between this speed-up approach and the previous approach
  - ✓ Performance evaluation on EAMD- encryption in the following case study example:
    - ➢ Data encryption of 1packet of 1500 Byte
    - ➢ 16-byte sensitive field in a 1 packet



If the data field that are sensitive are determined in advance, the encryption function can be realized on low resource IoT devices under severe realtime requirements (because of periodical process) by reducing uncecessary encryption process

2 - 7 X.iotsec - 1 study schedule

HITACHI
Inspire the Next

Timing	Place	study contents
2013/9	Korea	Propose EAMD mechanism as M2M security standard
2014/1	Switzerland	Recognize IoT security problems and the necessity of EAMD mechanism Confirm the necessity of ISO/IEC SC27 WG2 support
2014/6	Korea	Determine the scope of IoT security standard Clarify that the target is IoT device layer
2014/9	Switzerland	Establish a new work item in SG17 Send liaison documents to ISO/IEC SC27 WG2 and OneM2M WG4
2015/4	Switzerland	Confirm there is no overlap between standardization organizations based on the received liaison document
2016/3	Switzerland	Confirm the technical consistency of the whole draft
2016/9	Switzerland	Confirm by the governments and TSB(ITU-T central office)
2017/3	Switzerland	Plan to complete standardization and publish Recommendation[*1]

[*1]: The highest enforcement power standard weaker power standard is Supplement

HITACHI
Inspire the Next

Contents

1. Background
2. The status of standardization in ITU-T
3. The status of standardization in ISO/IEC JTC1
4. Summary

3 - 1 IoT security study in ISO/IEC JTC1 SC27

HITACHI
Inspire the Next

- What is ISO/IEC JTC1 SC27*?
  - ✓ committee specifying international standards on information security
  - ✓ 5 WGs
    - ➢ information security management systems（WG1）, cryptography and security mechanisms（WG2）, security evaluation standard（WG3）, security control and service（WG4）, identity management and privacy techniques（WG5）
- The status of IoT related project
  - ✓ In WG2, project 29192 on IoT-targeted cryptographic primitives is ongoing.
  - ✓ standardization projects are carried out for different purposes for different parts

purpose	Part
General	29192-1:General
（symmetric key）standard for data confidentiality	29192-2:Block ciphers 29192-3:Stream Ciphers
（public key）standard for entity authentication	29192-4:Mechanisms using asymmetric techniques
（symmetric key ）standard for data authentication	29192-5:Hash functions Study period: MACs

Hitachi's activity: standardization of Hitachi-developed mechanisms: Chaskey for MAC, Lesamnta-LW for hash, Enocoro for encryption

* under the committee(JTC1) that ISO and IEC established for information processing standardization

3 - 2 ISO/IEC29192 published standard

HITACHI
Inspire the Next

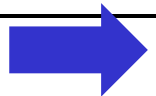
- ISO/IEC29192-1:2012 (General)
  - ✓ Terms, Criteria that should be satisfied by 29192standardcryptographic primitives (security strength not less than 80bits, hardware/software implementation requirement, maturity etc) are specified
- ISO/IEC29192-2:2012 (Block ciphers)
  - ✓ cryptographic primitives that enable hardware low resource implementation are specified: Present (64bits) and CLEFIA(128bits)
  - ✓ Simon and Speck have been proposed by U.S for the future revision
- ISO/IEC29192-3:2012 (Stream Cipher)
  - ✓ Cryptographic primitives that enable hardware low resource implementation are specified: Enocoro-128v2 (128 bits key), Enocoro-80 (80 bits key), Trivium (80 bits key)
- ISO/IEC29192-4:2013 (Mechanisms using asymmetric techniques)
  - ✓ Public key cryptographic primitives that enable low resource implementation are specified: cryptoGPS, ALIKE, IBS

ISO/IEC 29192-5 has NOT been published yet
⇒ standardization project on IoT-targeted lightweight hash function is on-going

3 - 3 The status of ISO/IEC 29192 standardization study

HITACHI
Inspire the Next

Timing	Place	29192-1	29192-2	29192-3	29192-4	29192-5	29192-6 (tentative)
2009/5	China						
2009/11	U.S						
2010/4	Malaysia						
2010/10	Germany						
2011/4	Singapore						
2011/11	Kenya						
2012/5	Sweden						
2012/10	Italy						
2013/4	France						
2013/10	Korea						
2014/4	Hongkong						
2014/10	Mexico						
2015/5	Malaysia						


: preliminary study

: standardization project study

3 - 4 ISO/IEC 29192-5 candidate mechanisms

HITACHI
Inspire the Next

- Lesamnta-LW
  - ✓ 256-bit hash function using a block cipher employing AES components
  - ✓ low RAM-used (50 Byte) implementation on 8-bit microcontrollers is possible
  - ✓ presented in ICISC 2010 conference and IEICE journal
    - ■On H8, low memory implementation that uses 54-byte of memory (RAM) was realized
      - ➢84% reduction in terms of memory, compared to the IT standard SHA-256

  Lesamnta-LW is the only candidate mechanism among IoT device targeted SW-oriented hash Developed by Hitachi Ltd., Univ. Kobe, Univ. Fukui, and KU Leuven (Belgium)

- Spongent
  - ✓ Sponge function-based hash function
  - ✓ hash length supports：80, 128, 160, 224, 256
  - ✓ Presented in CHES 2011 conference
  - ✓ Low-gate count (738GE) hardware implementation is possible
- Photon
  - ✓ Sponge function-based hash function
  - ✓ hash length supports：80, 128, 160, 224, 256
  - ✓ Presented in conference(CRYPTO 2011)
  - ✓ Low-gate count (865GE) hardware implementation is possible

3 - 5 Lightweight MAC standardization preliminary study in ISO/IEC

HITACHI
Inspire the Next

Timing	Place	Contents
2014/10	Mexico	Establish Study Period on lightweight MACs Provide information on software-targeted mechanism *Chaskey*
2015/5	Malaysia	Clarify the needs of lightweight MAC standard -Liaison statement from ITU-T SG17 points out that there does not exist lightweight MAC standard needed for connected car security -Confirm the difficulty of application of IT-MAC standard 9797 on IoT devices - Plan to establish standardization project at the India meeting last week

Implementation results：

- Achieve the speed of 7.0 cycles/byte on ARM Cortex-M4
  - Comparing to AES-128-CMAC, Chaskey achieves 12time higher speed, program size is 1/20

CPU	algorithm	Data size (byte)	Program size (byte)	Speed (cycles/byte)
Cortex-M4	AES-128-CMAC	128	8,740	89.4
	Chaskey	128	402	7.0

Chaskey (IoT-targeted software-oriented MAC) is the only studied mechanism
Collaboration development between KU Leuven(Belgium) and Hitachi Ltd.

HITACHI
Inspire the Next

Contents

1. Background
2. The status of standardization in ITU-T
3. The status of standardization in ISO/IEC JTC1
4. Summary

4 Summary

HITACHI
Inspire the Next

- Standardization going from lower device layer to upper application layer
- ITU-T standardization on IoT device-targeted cryptographic application techniques
  - ✓ Clarify problems with conventional IT cryptography when applied to IoT devices
  - ✓ Establish X.iotsec-1project on IoT devices
  - ✓ EAMD mechanism that copes with realtime requirement is the only mechanism
- ISO/IEC JTC1 standardization on IoT device-targeted cryptographic primitives
  - ✓ Published standard 29192-1, -2, -3, -4 on IoT device-targeted cryptographic primitives
  - ✓ The current discussions are on IoT device-targeted cryptographic primitive standard for data authentication
    - ➢ IoT devices -targeted hash function
      - – DISstandarddraft29192-5 is under review
      - – low resource (memory /circuit) SPONGENT, PHOTON, Lesamnta-LW are standard candidate
    - ➢ IoT devices -targeted MAC
      - – Confirmed the status of security and performance of Chaskey
      - – Plan to standard project on IoT devices -targeted MAC on October

Security countermeasures based on the combination of ISO/IEC standard and ITU-T standard expect to enable to install security functions on IoT devices under the severe resource requirements.

It might be interesting to discuss whether IETF de-facto standards can incorporate these de-jour standards to aim to improve the security of IoT systems in the future direction

Trademarks

HITACHI
Inspire the Next

- Enocoro and Lesamnta are trademarks of Hitachi Ltd.
- CLEFIA is a trademark of Sony Corporation.

HITACHI

Inspire the Next