HALT実験
Many standardization organizations start IoT security study since 2004

<table>
<thead>
<tr>
<th>Organization</th>
<th>Study Focus</th>
<th>Standards Developed</th>
<th>Other Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
• 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 cryptography standardization project: 29192
  - ITU-T SG17
    - IoT end-device security standardization project: X.iotsec
  - oneM2M WG4
  - 3GPP SA3
ESP
IP Authentication Header
Internet Key Exchange
Cryptographic Suites
Http over TLS
TLS protocols
TLS cipher suites
S/MIME Message Specification
Cryptographic Message Syntax
Cipher suits for generic purpose
Cipher suits for cloud computing
Cipher suits for lightweight apps.
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
EAMD protocol for IoT
IoT era comes!
データ分析

データを収集し、分析することで新たな洞察を提供します。
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
● 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
Reduce the overhead by encrypting the only data that are sensitive
Generate packet using the mask indicating sensitive data location

<table>
<thead>
<tr>
<th>Packet</th>
<th>Buffer (for temporary computation)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Packet Diagram" /></td>
<td><img src="image2" alt="Buffer Diagram" /></td>
</tr>
</tbody>
</table>
Packet storing process using the mask that has been shared in advance
206

・ 電磁気波である電波は、映像を伝送するためには信号を変調する必要がある。

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

\[ *G_{\text{DF}} + \text{UB}_F + \text{PO}_{\text{W}} + \text{UM}_F + \text{UP} \]

© Hitachi, Ltd. 2015. All rights reserved.
### Timing, Place, and Study Contents

<table>
<thead>
<tr>
<th>Timing</th>
<th>Place</th>
<th>Study Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/9</td>
<td>Korea</td>
<td>Propose EAMD mechanism as M2M security standard</td>
</tr>
<tr>
<td>2014/1</td>
<td>Switzerland</td>
<td>Recognize IoT security problems and the necessity of EAMD mechanism Confirm the necessity of ISO/IEC SC27 WG2 support</td>
</tr>
<tr>
<td>2014/6</td>
<td>Korea</td>
<td>Determine the scope of IoT security standard Clarify that the target is IoT device layer</td>
</tr>
</tbody>
</table>
| 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                  |
• 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

<table>
<thead>
<tr>
<th>purpose</th>
<th>Part</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>29192-1:General</td>
</tr>
<tr>
<td>(symmetric key )standard for data confidentiality</td>
<td>29192-2:Block ciphers</td>
</tr>
<tr>
<td></td>
<td>29192-3:Stream Ciphers</td>
</tr>
<tr>
<td>(public key )standard for entity authentication</td>
<td>29192-4:Mechanisms using asymmetric techniques</td>
</tr>
<tr>
<td>(symmetric key )standard for data authentication</td>
<td>29192-5:Hash functions Study period: MACs</td>
</tr>
</tbody>
</table>

© Hitachi, Ltd. 2015. All rights reserved.
ISO/IEC29192-1:2012 (General)

- Terms, Criteria that should be satisfied by cryptographic primitives (security strength not less than 80 bits, 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 (64 bits) and CLEFIA (128 bits).
- 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.
<table>
<thead>
<tr>
<th>Timing</th>
<th>Place</th>
<th>29192-1</th>
<th>29192-2</th>
<th>29192-3</th>
<th>29192-4</th>
<th>29192-5</th>
<th>29192-6 (tentative)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009/5</td>
<td>China</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2009/11</td>
<td>U.S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010/4</td>
<td>Malaysia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010/10</td>
<td>Germany</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011/4</td>
<td>Singapore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011/11</td>
<td>Kenya</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012/5</td>
<td>Sweden</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012/10</td>
<td>Italy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013/4</td>
<td>France</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013/10</td>
<td>Korea</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014/4</td>
<td>Hongkong</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014/10</td>
<td>Mexico</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015/5</td>
<td>Malaysia</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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
### 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

### 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

© Hitachi, Ltd. 2015. All rights reserved.
### [日本語]

このページには、日本語のテキストが記載されています。内容は日本語のテキストです。
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-1 project 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
● Enocoro and Lesamnta are trademarks of Hitachi Ltd.
● CLEFIA is a trademark of Sony Corporation.