Tool-less provisioning on ISA100.11a
Kazunori Miyazawa is a research engineer of Yokogawa Electric corporation. He received a master degree of mechanical engineering of Meiji University in March, 1999. He belong to Yokogawa Electric corporation from April 1999. He is a member of WIDE project from 2001. He developed Linux IPv6 IPsec stack and a key exchange application as a core member of USAGI project that deployed IPv6 on Linux community.

Currently he is a leader of PKI project of technical working group of ISA100 WCI.
Outline

- ISA100.11a architecture and provisioning
- Overview of Tool-less provisioning
- Router for Tool-less provisioning
- Feasibility Study
- Further study items
- Conclusion
ISA100.11a network architecture

Security and Keys of ISA100.11a

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Shared with</th>
<th>Generate or derive</th>
<th>Protect by</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL key</td>
<td>DL subnet</td>
<td>Security manager</td>
<td>Master key</td>
</tr>
<tr>
<td>TL session key</td>
<td>Communication End points</td>
<td>Security manager</td>
<td>Master key</td>
</tr>
<tr>
<td>Master key</td>
<td>Device and manager</td>
<td>From join key</td>
<td>Join key</td>
</tr>
<tr>
<td>Join key</td>
<td>Device and manager</td>
<td>Provisioning</td>
<td>Provisioning method</td>
</tr>
</tbody>
</table>
OOB provisioning depends on trustworthiness of a field worker

1) Provisioning

2) Share

3) Join

Field worker

Potential risks
- Install to another device
- Lost or steal handheld

Wireless Device

Router

BBR

Manager Gateway

UI

Operator
OTA provisioning secured with PKI

- Device Certificate
- Wireless Device
- Provisioning Network (Insecure subnet)
- Certificate Authority
- CA Certificate
- Manager Gateway
- UI

Join w/ K_global (public join key)

- Read certificate
- Challenge response
- Write a join key

Validation
Overview of Tool-less provisioning

1) Join provisioning subnet
2) OTA PKI Provisioning
3) Join operational subnet

Issues
• How to manage provisioning subnet?
• How to transport provisioning communication?

Restrictions
• Conformance with ISA100.11a
• Small foot print
Device internal model of ISA100.11a has a restriction

- Reference model
  - Application process
    - Set of objects
    - Communication Endpoint
  - Object
    - Set of attributes
    - Interface of attributes
  - Attribute

- DMAP
  - 1 subnet ID
  - 1 128 bit address
  - 1 16 bit alias address
  - Port number is fixed

- NLMO route table
  - Interface field is Boolean type
    - 0 is DL, 1 is backbone

Ref: ISA100.11a:2011 Page 90, Figure 25 – Example of management SAP flow through standard protocol suite
2 DMAP model

DMAP for provisioning network

DMAP for operational network

DAR (Dual Advertisement Router) internal model

Ref: ISA100.11a:2011 Page 84, Figure 16 – Reference model
Feasibility study
Conformance of DAR stack with ISA100.11a

• We confirmed that Tool-less provisioning is feasible with conforming to ISA100.11a standard.
  – Interoperable ISA100.11a products (YTA 510)

• We only needs extra communication resource assignment by a system manager.
  – No protocol extension

• What resources are assigned by the manager is depends on a system and it is out of scope of the standard.
Demonstration
Further study items

• Optimization
  – Proposed Tool-less provisioning architecture focuses on conformance with the ISA100.11a standard.
  – If revising the standard is acceptable, we can optimize the architecture to reduce footprint, bandwidth, energy consumption and so on.

• Automate commissioning
  – Tool-less provisioning allows a wireless device to be able to join a system at network level without manual configuration.
  – However a wireless device requires application configuration to work in a control system. Automate the configuration leverages feature of Tool-less provisioning and contribute to achieve “Lick and stick sensors”.
Conclusion

• OOB provisioning is depends on trustworthiness of a field worker who operates a provisioning device.
• Tool-less provisioning is required from the security point of view.

• Standardization of ISA100.11a is almost concluded and revising to support Tool-less provisioning is unacceptable.
• This presentation shows feasibility of Tool-less provisioning with conformance to the ISA100.11a standard.

• Tool-less provisioning contributes not only security of wireless network system but also life-cycle excellence because it automates provisioning work and reduces expertise.
Thank you for your attention