SDPM: Secure Data Processing Model for NUI-NUX Environments

2014. 06. 02

Jae Dong Lee
SeoulTech
(jdlee731@seoultechackr)
Table of Contents

• Introduction

• Related works

• Secure Data Processing Model for NUI-NUX Environments (SDPM)
  – Architecture
  – Data processing
  – Service scenario

• Conclusion
Many products with cutting-edge UI/UX technologies are now being released as wearing devices, such as bands, glasses, watches, and clothes.

Various devices - a video camera, range camera, GPS, and microphone, also enable users to obtain information, such as speed, temperature, pressure, and humidity, through sensors.

By processing various data, these devices provide convenient user services that were previously impossible to obtain at one time.

NUI-NUX data are indirect personal information because they contain individuals’ current conditions, locations, propensities, and tastes.

If NUI-NUX data are combined with direct personal information, such as names, IDs, and resident registration numbers, serious personal information leakage may occur.
The proposed scheme provides selective security reinforcing functions for highly sensitive data by cryptographic means such as authentication, encryption, and security channels while maximally ensuring data availability to avoid deterioration of performance during NUI-NUX data processing.
Related work
Characteristic of NUI/NUX Data

• Heterogeneous
  – Although not considered in previous devices that processed single sensors or modules, data having diverse sizes, frequencies
  – Characteristics should be processed by NUI-NUX equipment that must process data generated by diverse devices and sensors

• Real time
  – When the user uses a device in which many sensors and devices are combined, the scheme to store NUI-NUX data in the disk and load and process the stored content cannot satisfy the minimum performance for normal operation
  – NUI-NUX data should be processed in real time in the memory

• Data sharing
  – For the quality of rich NUI-NUX application services, data sharing is a prerequisite
  – Although the values possessed by single data are important, high-quality service cannot be provided with only single data processing
  – The correlations among diverse data should be analyzed
Characteristic of IoT environments

• IoT is composed of humans, objects, and services

• The structure of IoT can be divided into three layers
  – Perception layer: Receives signal inputs from various sensors
  – Network layer: Transmits the data from the perception layer
  – Application layer: Provides diverse services and interfaces through the data transmitted from the network layer
Security requirements of NUI-NUX data processing (1/2)

• **Confidentiality**
  – Privacy information - current states, locations, tendencies, preferences is low level threats
    • But if the information is added with id, name, social security number
      – Can be critical privacy information
  – Selective confidentiality should be provided for protection of privacy invasion

• **Integrity**
  – The data sent by the transmission side and the data received by the receiving side should be identical without fail
  – To protect integrity during data transmission, measures
    • E.g. Authentication, Encryption, Security channels
  – The integrity of the existing stored data should also be protected so that unauthorized data changes would not be allowed
Security requirements of NUI-NUX data processing (2/2)

• **Availability**
  – Data availability should not deteriorate during data processing due to delay time and bottleneck phenomena resulting from the realization of confidentiality, integrity, and authentication
  – Users’ natural interfaces are the most important in NUI-NUX environments, and thus sufficient availability should be ensured

• **Authentication**
  – To prevent the success of attacks such as Man in the Middle attacks and Spoofing, a process to check whether the user is an authorized user through authentication before the user accesses important information is indispensable
Secure Data Processing Model for NUI-NUX Environments (SDPM)
SDPM - Architecture

Application Layer
- Classification
- Secure Mode
- Normal Mode
- Preprocessing
- NUX Collector

Middleware

Network Layer

Collection Layer
- Camera
- Microphone
- Collection Gateway
- RFID
- GPS
- Sensors
SDPM - Data processing

Preprocessing → Classification → Processing

Secure Mode
Normal Mode
SDPM - Data processing

- Secure Mode

<table>
<thead>
<tr>
<th>Hardware ID</th>
<th>Mode</th>
<th>Authentication</th>
<th>Data Encryption</th>
<th>Secure Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>#00000101</td>
<td>Secure</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>#00000202</td>
<td>Normal</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>#00000303</td>
<td>Secure</td>
<td>TRUE</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>#00000404</td>
<td>Normal</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>#00000505</td>
<td>Secure</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

Levels: Level 1: Authentication, Level 2: Data Encryption, Level 3: Secure Channel
SDPM - Service scenario (1/2)

• Definition of Acronyms

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>Collection module</td>
</tr>
<tr>
<td>PM</td>
<td>Preprocessing module</td>
</tr>
<tr>
<td>CLM</td>
<td>Classification module</td>
</tr>
<tr>
<td>SMM</td>
<td>Secure mode module</td>
</tr>
<tr>
<td>NMM</td>
<td>Normal mode module</td>
</tr>
<tr>
<td>NCM</td>
<td>NUX collector module</td>
</tr>
</tbody>
</table>
1 : Req_transfer()
2 : Rnt_transfer
3 : Req_Classification()
4 : Rnt_Classification
5 : Req_SecureMode()
6 : Rnt_SecureMode
7 : Req_Collection()
8 : Rnt_Collection
9 : Req_SecureMode()
10 : Rnt_SecureMode
11 : Req_NormalMode()
12 : Rnt_NormalMode
13 : Req_Collection()
14 : Rnt_Collection
Conclusion
Conclusion

• A secure scheme was proposed that can respond to Man in the Middle attacks, Spoofing, and evasion of authentication

• To prevent the occurrence of bottleneck and delay phenomena
  – Important problems when NUI-NUX data are processed, the proposed scheme primarily enables designating the devices
  – Require the security mode and applying the secure mode to those devices

• The proposed scheme enables selectively applying encryption and security channels in the secure mode

• Data processing technologies should be studied further taking into consideration certain situations and authorities applied with access control technologies

• In addition, methods for judging whether to apply content-based security should be studied
References

• Shancang Li, LiDaXu, Xinheng Wang. Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS 2013; 9(4): 2177–2186


Q & A