AMI Topology and its Security

Manish Shrestha
Overview of Electricity Grid

• Generation
• Transmission
• Distribution

Figure 1.1. Simplified representation of the physical electric power system
Smart Grid
Some Communication technologies in Smart Grid

• Wireline technologies
  • PLC
  • DSL
  • Fibre Optic

• Wireless Technologies
  • IEEE 802.15.4 (Zigbee, ISA 1000.11a,...)
  • Wi-Fi
  • WiMAX
  • GSM (2G, 2.5G, 3G...)
  • EN 13757 (Wireless m-bus)
<table>
<thead>
<tr>
<th><strong>EN 13757</strong></th>
<th><strong>Propose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Basic data communication between meters and collectors</td>
</tr>
<tr>
<td>2</td>
<td>Physical layer requirement for wired M-bus</td>
</tr>
<tr>
<td>3</td>
<td>Application Layer</td>
</tr>
<tr>
<td>4</td>
<td>Physical and Data Link Layers for wireless M-bus</td>
</tr>
<tr>
<td>5</td>
<td>Relaying and routing for range enhancement</td>
</tr>
<tr>
<td>6</td>
<td>Local bus for short distance wired links</td>
</tr>
</tbody>
</table>
• Smart meter
• Concentrator
• Head-end system
• MDM system
• NAN
• Cellular networks
Omnia Nework
Utilidriver
Flow of Information
Attack Interface

- Open Ports
- Default Settings
- Radio Network
- Cellular Network
Assets to protect

• Physical Ports
• Stored metering data (consumption, logs, alarms)
• Encryption keys
• Communication channel
• Firmware/updates
• API
• Physical location
What can we do?

• Proper key management
• Incident response, user training and awareness
• Use of private APN
• Physical Security and tamper detection
• Update/patch management
• Follow guidelines and best practices from designated organizations.
• Proper configuration
• Defence in Depth
Conclusion

• Several security risks exist
• Need of certification or minimum concrete standards requirements before choosing the vendors
• DSO collaboration with research institutions
References


• Kamstrup Documents http://www.products.kamstrup.com

