Update on DNP3 Secure Authentication

Grant Gilchrist
## Secure Authentication Versions

<table>
<thead>
<tr>
<th>Ver</th>
<th>Date</th>
<th>Description</th>
<th>Use?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2007-01-31</td>
<td>Initial release</td>
<td>No</td>
</tr>
<tr>
<td>2</td>
<td>2008-07-31</td>
<td>Revision after review by initial implementers. <em>Included in IEEE Std.1815-2010</em></td>
<td>YES</td>
</tr>
<tr>
<td>3</td>
<td>2010-03-17</td>
<td>Revision after cryptographic review by Information Trust Institute at University of Illinois. First non-draft release to permit remotely changing Update Keys and include security statistic objects.</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>2011-02-25</td>
<td>Revisions to version 3 after review by initial implementers</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>2011-11-08</td>
<td>Revisions to version 4 after review by Smart Grid Interoperability Panel Cyber-Security Working Group. <em>Included in draft of IEEE P1815-2012</em></td>
<td>YES</td>
</tr>
</tbody>
</table>
What's Wrong with v3 and v4?

- Implementers found interoperability problems with v3
  - Some situations not clarified
  - Combinations of situations not handled
  - Restart sequence not well-described

- SGIP Cyber-Security Working Group looked at v4 as part of reviewing IEEE 1815-2010
  - Wanted to see if missing items were being addressed
  - Found problems with remotely changing Update keys
  - Was sending the same data encrypted and non-encrypted
  - Open to brute-force attack on keys
  - Fix is to replace encryption with message authentication code (MAC)
Changes Between Ver 2 and Ver 5

- Added ability to remotely change keys, maybe using certificates
- Review by Information Trust Institute, U. of Illinois
  - Throttle sending error messages
  - Avoid changing session keys too often in response to errors
  - Measure and report security statistics
- Comments from implementers
  - Clarify how to authenticate “aggressive mode” confirmations
  - Calculate challenge sequence numbers differently **not compatible**
  - Initialize session keys immediately after restarts
- Review by SGIP CSWG
  - Increase strength of cryptographic algorithms
  - Add AES-GMAC as a MAC algorithm
  - Vulnerability in remote key change mechanism
SAv5 was released November 9, 2011

- [http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf](http://www.dnp.org/Lists/Announcements/Attachments/7/Secure%20Authentication%20v5%202011-11-08.pdf)

- Unlike previous specs, available even to non-members

- Formatted Chapter 7 of the draft IEEE P1815-2012

- Accompanied by an announcement

  - Version 1,3 and 4 are withdrawn
  - SAv2 is deprecated and should not be deployed in new implementations
  - SAv2 and SAv5 are not compatible
  - SAv5 will be included in IEEE Std. 1815-2012
Concerns from Announcement

- Many spec changes in a short period of time
- Announcement was very concise, perhaps cryptic
- A few vendors had only just released SAv2
- Concerned about meaning of term “deprecated”
- Worried about investment in current projects
Clarifying Announcement

- Sent out last week (Dec 2, 2011)
- No need to remove, replace or update existing SAv2 systems
  - SAv2 is still better than not implementing security
  - Finish your current procurement process
  - Use SAv2 until SAv5 implementations are available
  - Move to SAv5 as soon as possible
- Devices with *only* SAv5 cannot talk those with *only* SAv2
- However, a device may talk SAv5 to one device, SAv2 to another
- Explains why these changes were made
- Explains that security is constantly changing
- A program for releasing security updates is coming soon