IEEE PSCC S3 SG: Draft Standard for Interoperability of IPSEC Utilized within Utility Control Systems

Chair: Jim Bougie
Vice Chair: Marc Lacroix
Secretary: James Formea
Output: Ballot resolution
Established:

Summary Minutes for Subcommittee Report
The S3 SG meeting was held on Monday, September 11, 2017 with 14 attendees.
The goal of this meeting was to discuss the comments to complete the ballot resolution.

Purpose of S3 SG:
The purpose of this document is to define specific configuration profiles of the Internet Protocol Security (IPsec) protocol suite suitable for use within a utility control system. The primary goal in developing this standard is to promote interoperability between products developed by different vendors. It focuses on those configuration parameters needed to support the establishment and sustained operation of an IPsec Virtual Private Network (VPN) tunnel between two devices which have implemented IPsec conforming to this standard. A secondary goal of this standard is to minimize configuration errors involving IPsec implementations within utility control systems.

Request for January 2018 S3 plans to meet as a Task Force in a single session for 20 people and a computer projector.

After the patent slides review, James Formea started the review of the unresolved comments.

Comment #1: There was a lot of discussion on the support of multicast communication. According to Herb Falk, GDOI or shared keys must then be used. Another approach is to use self-manage that presents the advantage of being convertible to certificate base system.
Richard Corrigan will prepare a description of self-manage key.

Comment #2: Support for IKEv2 only.

Comment #3: The next draft will include the information

Comment #4: Three AES algorithm will stay. 3DES is not included.

Comment #5: Further clarifications are needed. James Formea will contact Colin Gordon

Comment #6: Clarification will be added to the text

Comment #7: Other expertise is needed to solve this comment

Comment #11: Crypto export restriction is managed by manufacturer

Comment #12: A table will be added to the document to summarize the vendor compliance.

Issue: The group seemed to drift away from the original intent of documenting/standardizing the Lemnos IPsec profile because it is no longer considered "secure enough" due to the use of pre shared keys and Diffie-Helman group 5... I'm still on the fence about whether or not we should preserve a "Lemnos compatibility" profile and then include a stronger profile to be recommended for new installations, or if we should abandon the existing Lemnos profile that is in the draft today and focus only a more secure profile. The trouble I have with the latter is that we really have no basis on which to say that this new profile will be an interoperable profile, because we will have no idea if anyone is actually using the same set of chosen options.

Actions items

1) Richard Corrigan to prepare a description of self-manage key
2) James Formea to contact Colin Gordon (comment #5)
3) James Formea to find experts to help solve comment #7