February 24, 2021
Webinar Questions and Answers

"Synchrophasor Cybersecurity for Grid Operations" with Scott Mix

Question: How do archive walker supports for Synchrophasor data analytics?

Answer: The author is not in a position to answer this question at this time.

Question: There are various difficulty in handling synchrophasor data any specialized software to perform Data analysis?

Answer: The author is not in a position to answer this question at this time.

Question: Compromising data is quite common problems now a days, how to secure the data?

Answer: Protocols that support tamper detection, for example by assigning a cryptographic hash to the data can allow the receiver to be aware of any tampering that occurred and take application-specific action, such as disregarding the tampered data, and treating it as unavailable until the tampering has cleared (supporting integrity above availability). If the protocol doesn't support hashes directly, it could be "wrapped" inside of another protocol that does. The recently approved IEEE 1711.2 standard provides this for serial (non IP-based) communication, and IPsec protocols can be used for IP-based communication providing a secured "tunnel" within which the unprotected exchanges are passed. Note, however, that while IPsec can be used to secure UDP transfers, it requires bi-directional communication to manage the secured tunnel, and could not be used to secure end-to-end communication through a data diode (see later question). It would be possible to establish an IPsec tunnel initiated at the external interface of the data diode to protect the transfer at its more vulnerable point.

Another approach would be to implement transport layer security (TLS) version 1.2 or 1.3 (1.2 supports integrity without encryption, while 1.3 only supports encryption which includes integrity) using an approach similar to how IEC 61850 protects communication as described in IEC 62351-3 and IEC 62351-6.

Question: What are the lessons from Solar Winds incident for utilities and vendors?

Answer: The author is not in a position to answer this question at this time.

Question: What is the current state of the industry in terms of encryption of real time data sent by the PMUs. Are the standards like group encryption key exchange (GDOI) widely used and what are the plans in this regard?

Answer: This is a rapidly moving area for investigation and application. I don't have any direct knowledge of the current state of the industry. The IEC 62351-9 standard specifies the use of transport layer security (TLS) for authentication and optional encryption of data. TLS encryption requires exchanging of keys, using X.509 digital certificate and public key infrastructure to exchange keys. This work well for exchanges between two participants but can become a key management issue when communicating the same message to multiple endpoints (i.e., multicasting). The Group Domain of Interpretation (GDOI) protocol is the recommended approach for managing and distributing keys used for group (multicast) communication. GDOI implementations use an additional component, called a key distribution center (KDC) to manage the keys used to encrypt the multicast communication.

In terms of PMU communication, I imagine that the most prevalent method, especially for wide-area exchanges (PMU to PDC or PDC to PDC) is point to-point communication, implying that group keys would not be necessary so GDOI would not be needed; however, in cases where multicast is used it may be necessary.

Question: Can you comment about implementing a data diode for synchrophasor data transfer communications?

Answer: Data diodes are an appropriate method of protecting the PMU as long as there are no communication control responses needed. Simple streaming of data from the PMU to an external source (like a PDC) should be fine if using an unacknowledged protocol like UDP, but if an acknowledged protocol like TCP is used, or the data being streamed can be modified from the external source, for example, by selecting or deselecting different streams, or requesting filtering of the streamed data, the data diode will prevent the TCP acknowledgements or the modification commands from reaching the PMU (some data diode implementations can respond with TCP acknowledgements to emulate end-to-end communication, but cannot do anything about the stream modification commands which would need to be passed through). If end-to-end cryptographic methods are used, key management will need to be a manual or out-of-band process.

Question: How can fallback control options be designed for critical functions, when a cyber-intrusion or an OT anomaly is detected? Does any standard provide guidelines on this?

Answer: I'm unaware of any standards, but an application could be designed to flag tampered or suspect data as unreliable or unavailable, and use alternative sources, such as SCADA data or data from the other end of a line or another source on the same connected bus (if either are available). The exact processing would be dependent on the application objective.

Question: These are all very generic. Need to have some concrete suggestions/guidelines related to PMU use in real time operations.

Answer: The issue with specific suggestions is that they are heavily dependent on the equipment, network environment, and corporate environment. An effective security program should be crafted taking all of those into account.

Question: Considering that our devices have limited storage and computation power, is there a lightweight method for storing sensitive data such as keys and passwords inside those devices? Or do you recommend any other solution than storing them inside the devices?

Answer: The concept of a hardware security module (HSM) would be able to store the keys securely, but it would need to be designed and built into the devices. These devices have historically been expensive and require hardware support, but recent advances have decreased the cost, and USB-attached HSM devices are available to decrease the amount of hardware support (and therefore equipment cost) required for implementation. In either case, software support in the PMU or PDC is still required for accessing and maintaining keys on the HSM.

Question: The industry is struggling of real-time decision-making use of PMU, mainly due to CIP requirements and compliance. I expect to see more concrete guidelines in that regards.

Answer: There were several joint NERC/NASPI activities that attempted to provide additional guidance in applying the NERC CIP standards to synchrophasor and PMU environments, but they failed due to lack of consensus on how to implement the requirements.

When synchrophasor data is used to make real-time decisions, the data should be treated no differently than other telemetered data, and the PMUs should be treated no differently than similarly configured RTUs. An RTU in a substation that meets the criteria for protections under NERC CIP (for example, if the RTU is at a medium impact station, and the telemetry uses a routable protocol such as DNP3/IP) should have the same protection obligations as a PMU at the same location of the data is used for real-time applications.

Question: What is the biggest threat from a malicious attack on PMUs and what is the most important mitigation?

Answer: This is largely application dependent. If the attack is against a data source used in a remedial action scheme, it could cause reliability or security issues (triggering when it should not, or not triggering when it should). The operational impacts of that should be part of the RAS design process. On the other hand, if the application is situational awareness or forensic in nature, such as oscillation detection, there are likely few operational impacts.

I would venture that the most serious threat would be to a high-speed protection application (RAS or local) operating faster than human speeds or without supervisor oversight that could result in human or equipment safety compromises if the data were compromised.

Question: is there a practical application that differentiates cyber attack based missing data (PMU) and missing data due to a PMU device failure

Answer: In my opinion, the source of data unavailability doesn't matter to the application; the application must be able to appropriately account for the lack of data and either not take action, or switch to alternate sources for data. A device failure would tend to be permanent, while a cyber-attack that results in data loss may self-correct after the attack is over.

A bigger concern is the lack of data integrity that a cyber attack could cause by intentionally sending properly formatted false data to the application. The application would see a constant stream of data, but would not have correct data with which to make decisions, and not be able to determine that the data was incorrect. (Note that a mis-calibrated PMU or a drifting instrument transformer may produce similar results, and would be equally difficult to detect.) The adage "a man with one watch always knows what time it is; a man with two watches is never sure" applies here when there are a limited number of

data sources. Statistical analysis of multiple data sources (like those used in a State Estimator bad data detection and correction algorithm) may be able to help, but would require additional diverse PMU data sources to perform the analysis.

Question: May I get support to work with phasor data for analysis

Answer: The author is not in a position to answer this question at this time.