



PNNL-SA-183091

STTP Communications and Security

April 5, 2023

Scott R Mix, CISSP



PNNL is operated by Battelle for the U.S. Department of Energy



Overview

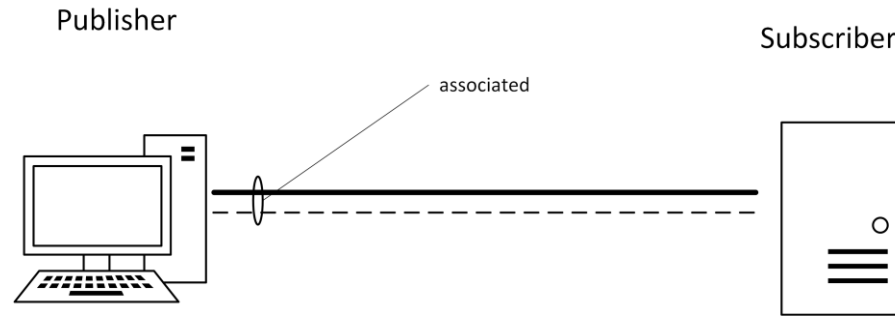
Streaming Telemetry Transport Protocol – STTP (IEEE Std. P2664)

- Communications Architectures
- Cybersecurity Considerations

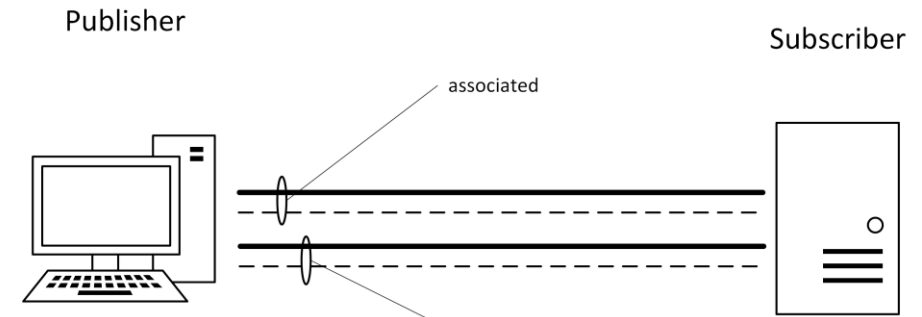
Communications Architectures

- Publish / Subscribe architecture
- Subscriber requests data from Publisher
- Publisher responds with data
 - Data can be real-time or historical, and can be filtered
- Combination of reliable connection (transmission control protocol - TCP) and unreliable connection (user datagram protocol - UDP)
 - Reliable connection required to establish session between Subscriber and Publisher
 - Reliable connection for STTP commands (data requiring acknowledgement [e.g., key exchange] or enforced delivery order)
 - Unreliable connection for data transfer (no acknowledgement or retry, but more efficient)
 - Reliable connection can also be used for data exchange, but uses higher communication overhead (and therefore lower throughput)
- Both reliable and unreliable connections can be encrypted

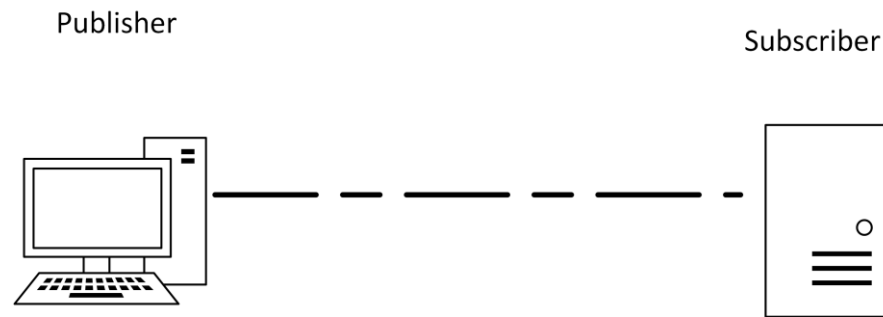
Communication Architectures



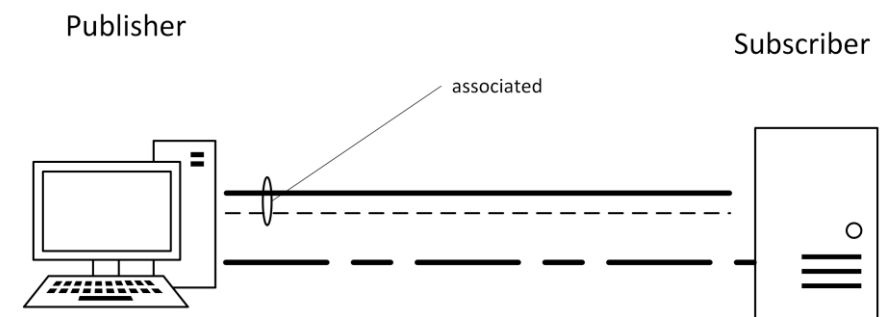
TCP Command Channel and UDP Subscription Channel






Two sets of TCP Command Channel and UDP Subscription Channel



Combined TCP Command and Subscription Channel



TCP Command Channel and UDP Subscription Channel with separate Combined TCP Command and Subscription Channel

	command channel – TCP connection used for reliable communication between publisher and subscriber
	subscription channel – UDP channel established to transmit data from the publisher to the subscriber
	combined command and subscription channel – TCP connection used for reliable communication between publisher and subscriber that includes data

Cybersecurity Considerations

- Command Channel
 - Establishes an STTP Session
 - Uses inherent TCP features for data integrity (TCP checksums) and out-of-order or missing packet (sequence numbers) detection and recovery
 - Acknowledgement of received data (retransmission of bad or missing data)
 - Supports Transport Layer Security (TLS)
 - ✓ Identity and authentication through standard Public Key Infrastructure (PKI) mechanisms
 - ✓ Provides confidentiality protections (when used, encrypting “ciphers” are required)
- Subscription Channel
 - Uses UDP – no automatic checking for integrity, packet order, or missing packets
 - No data acknowledgement
 - Identification and authentication tied to associated Command Channel (STTP Session)
 - Optional confidentiality using STTP encryption
 - Enabling UDP header checksums is strongly encouraged
- Combined channels
 - Same as Command Channel (TCP connection)

Cybersecurity Considerations

- Data Compression
 - Specifies GZIP (default) for UDP Subscription Channel and Time Series Special Compression (TSSC – see code in Annex C) (default) for TCP Subscription Channel
 - Other algorithms can be negotiated if both Publisher and Subscriber support them
- Forward and Reverse Connections
 - Publisher generally located inside of security enclave (e.g., in a substation or a control center)
 - Required “forward connections” used when Subscriber initiates the connection to the Publisher to request (pull) data
 - ✓ Subscribers can be brought up or taken down as needed
 - Optional “reverse connections” used when Publisher initiates the connection publish (push) data to the Subscriber
 - ✓ Used when Publisher is in a security enclave that must initiate all data transfers
 - ✓ Subscribers must always be available to receive data from the Publisher

Cybersecurity Considerations

- VPN tunnels also supported
 - VPN processing handles data integrity and confidentiality issues
 - Useful for site-to-site connections where routers handle all encryption and internal communications do not need to be encrypted
 - Hardware acceleration for encryption (and possibly compression)
 - TLS can still be used for identification and authentication inside the VPN, but TLS encryption is not necessarily required
 - Can inherently provide integrity checking for Subscription Channels
- Access Control
 - Access Control Lists (ACL) maintained by Publishers
 - ✓ Uses a measurement's unique identifier
 - Access Control Lists should conform to filter expressions (described in Annex C)
 - Publishers can also deny requests from Subscribers

Cybersecurity Considerations

- Encryption
 - Recommend that the Command Channel (TCP) use TLS (with encryption)
 - Self-signed digital certificates are supported
 - Subscription (Data) Channel (UDP) can be encrypted by STTP using symmetric keys
 - ✓ AES256 by default; others optionally supported
 - Command Channel encryption using TLS is **STRONGLY RECOMMENDED** if the UDP Subscription Channel is also encrypted, since the UDP encryption keys are exchanged over the Command Channel
- Encryption Key Management
 - TLS specification includes key refresh commands, but it is not universally implemented
 - ✓ If refresh implemented, it should be specified for at least every 4 hours
 - STTP Subscription Channel key refresh provides for two keys, one in use at a time (as identified in a Command Channel message)
 - STTP Subscription Channel key refresh is specified for every four (4) hours



Thank you

