Aeron Transport Security (ATS)

Aeron
Sponsored by Adaptive

A data packet traverses many systems on its way to a destination, introducing risk that the content may be seen by unintended parties. The Internet Engineering Task Force (IETF) considers pervasive monitoring an attack which should be mitigated by security protocols like encryption and message authentication when possible.

However, in trading applications, these protocols create latency, making compromises necessary. This increased information security may be less necessary when the data environment is on a single premises with only one entity in control, such as an exchange co-location. For applications on the cloud, or those whose packets travel through the internet, the latency may be a necessary compromise. **These circumstances demand the highest protection possible with the least latency.**

Introducing Aeron Transport Security (ATS)

Aeron is a messaging transport protocol that operates in a variety of environments, from local server based to cloud native deployments. **Aeron Transport Security (ATS)** secures Aeron frames on the network with industry-proven technologies. ATS extends the Aeron protocol to add:

- **Lightning fast, industry-leading OpenSSL cryptography**
  Standard across countless industries, OpenSSL uses the power of modern hardware to enable ATS' superior performance.
- **"Secure by default" design**
  Aeron publications and subscriptions are secured by default unless opted out.
- **Secure streams**
  ATS supports unicast, multicast, and multi-destination-cast.
- **Public Key authentication**
  Each ATS-enabled driver has a public/private key pair and can be configured with other public keys for other drivers. Communication between ATS-enabled drivers is only allowed if each driver is aware of the other's key and passes signature validation.

Technical Details

Driver RSA public/private key pair

- Generated by user and configured via PEM format files for easy integration into key management systems.
- Key length and parameters controlled by administrator.

Each Aeron stream is secured by

- An Elliptic Curve Diffie Hellman Ephemeral (ECDHE) key pair generated for the stream endpoints individually which is re-keyed upon termination of either end.
- An HKDF RFC 5869 key derivation function.
- An AES_256_GCM_SHA384 cipher suite providing Authenticated Encryption with Associated Data (AEAD).

Operational Considerations

- Supported in the Aeron C driver only
- OpenSSL 1.1.1 dependency.
- Available as an Aeron Premium feature.

Behind Aeron

Adaptive builds & operates bespoke trading technology solutions across asset classes for financial services firms wanting to own their tech stack to differentiate and compete in the long-term. Central to Adaptive's offering is Aeron, the global standard for high-throughput, low-latency and fault-tolerant trading systems - the open-source technology supported and sponsored by Adaptive.