Mueller AMI Safety & Security

Security

As the number of connected devices increase, and user expectations expand, the challenge of providing highly secure and reliable systems becomes more and more complex—yet absolutely essential. Mueller understands security and make it a part of everything they do. It is more than just protecting data or securing devices and communication networks—it is adopting policies and processes and investing in people that make security a priority. Mueller takes a holistic approach to cybersecurity. Security processes and policies, rooted in the NIST Cybersecurity Framework, and aligned to ANSI/AWWA G430: Security Practices for Operations and Management, exemplify best practices from across industries. Software development is also guided by cyber security best practices including OWASP and SANS SWAT.

Mueller provides *Annual Commercial Security Briefings* because they believe in sharing their security expertise with their utility partners. *Quarterly Internal Testing, Security Audits, and Vulnerability Reviews* keep customers informed on how Mueller has responded to changes in the security landscape, both within the industry and beyond. Yearly, *Third-Party Penetration Testing* (software, hardware, devices, network, and infrastructure) ensures the system remains safe and strong. Mueller's *Product Security Incident Response Team* (PSIRT) regularly rehearses responses to various cyber-attacks, maintains a response playbook, and is always ready to help customers respond to any threat or incident that does occur using encrypted communications for added security.

AMI Communications Security

Robust communication protocols guard against eavesdropping and data loss between Mi.Net® endpoints, collectors, and Sentryx. Mi.Net endpoints are programmed with individual, unique keys at time of manufacture. Unique keys mean every endpoints has its own unique encryption. These keys are used to generate AES-128 session keys for joining the network, signing and encrypting control messages down to the node from the network, and to sign all upstream messages. Packets contain a 16-bit Cyclic Redundancy Check (CRC) to ensure data and message integrity. Any packet that arrives at the network server which fails a CRC check, or fails the network signature check is rejected, and not processed by the network server, nor forwarded to the application server. If the keys become compromised, new keys can be generated for that Mi.Node™ by having it rejoin the network. Keys are never transmitted over the radio network, or between collectors and the network server.

The Mi.Net® system also incorporates industry leading security features for remote disconnect commands. This methodology was developed in concert with a 3rd party cyber-security firm, hired by one of the largest water utilities in the United States. These features include the ability to require users to re-authenticate to initiate disconnect or reconnect commands and throttling procedures to safeguard against mass commands sent from an individual user account accidentally or with malicious intent. More importantly, in addition to the unique security keys referenced above, each individual disconnect command receives a digital signature which can't be reused, eliminating the threat of "copy-cat" commands. Mueller's leading position as the industry's only proven supplier of remote disconnect meters has allowed them to also lead the industry in RDM security protocols.

Network and Software Security

Traffic between network collectors, the network provider server, and the Sentryx application server all utilize HTTPS to guarantee security and message delivery (at the TCP level). Messages that fail transmission are cached or stored at the appropriate level and delivered later when communication has been restored. If there is a persistent communication error between the collector and network server, or network server and the application server, the data is able to be retrieved at a later time.

The Sentryx user interface utilizes parameterized queries to access data from the database which prevents SQL injection from untrusted user input. The user interface also utilizes input validation to protect from cross-site scripting attacks. Sentryx is also protected by an industry standard Web Application Firewall, Intrusion Prevention, and Intrusion Detection System that is monitored twenty-four hours a day, seven days a week.

All Sentryx application servers are fully backed up weekly, with incremental backups daily. Sentryx database servers are fully backed up weekly, with incremental backups every other day. The database logs are backed up every 30 minutes, allowing a database restore to occur for a time period granularity of 30 minutes.

Access to data within Sentryx is securely controlled through rights/privileges, from single account viewing to full administrative rights. Setnryx utilizes parameterized queries to access data from the database which prevents SQL injection from untrusted user input. The user interface also utilizes input validation to protect from cross-site scripting attacks.

Our cloud hosting provider, INAP, a Tier 3, SOC 2 Type II data center, maintains Web Application Firewalls, Intrusion Prevention Systems, and Intrusion Detection Systems, and other technology to constantly monitor for Denial of Service (DoS) attacks and other potentially malicious activity, and alerts Mueller of any potential threats. Mueller is able to proactively protect against DoS through traffic filtering before the traffic reaches the Sentryx applications and data.

Software and Network Security Including:

- Web Portal
  - 2048 bit RSA SSL Certificate
  - TLS 1.2
- Over-The-Air Encryption
  - Advanced Encryption Standard (AES) 128 bit keys
  - Unique keys per individual node
  - All messages encrypted and signed bi-directionally
- Collector to Server Communication
  - Private APN over 3G
  - Not accessible over the internet
  - Private VPN to Mueller Systems servers – AES 256-bit key
- Server Network Infrastructure
  - IDS / IPS / WAF
  - Tier 3
  - SOC 2 Type II