Leading-Edge Security for AMR/AMI Systems

A WHITE PAPER BY NEPTUNE TECHNOLOGY GROUP INC.

As AMI and AMR systems have become more complex and feature packed, they have become a more enticing target for hackers looking to do harm to your utility. From simple theft of water due to rising prices or conservation efforts, to attacks looking to take over or disable your distribution system, every piece of the connected water utility needs to be evaluated for security and proper controls need to be implemented. It is critical to place a high priority on identifying and eliminating vulnerabilities and risks at every point within your systems in order to help ensure that your utility remains safe.

All Neptune® products are designed with security as a top priority. All coding is done with OWASP (Open Web Application Security Project) best practices in mind and utilizes techniques such as prepared statements, input validation, Transport Layer Security, and encryption or hashing where appropriate. All databases are authenticated and encrypted at the file level to prevent unauthorized access to your data. All sensitive data, such as passwords stored within our databases, are separately encrypted or hashed and salted to further protect from theft or malicious use. Communications between field devices and the host system are protected by the use of Federal Information Processing Standard (FIPS) 197 compliant encryption or better.

STRENGTHENING SOFTWARE SECURITY IN PRIVATE CLOUDS

Neptune utilizes Amazon AWS for all Software-as-a-Service (SaaS) products. This allows us to leverage the security that Amazon has built into its datacenters and online services to bolster the security profile of our cloud-based offerings. Amazon has achieved ISO 27001 certification and has been validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS) with annual Service Organization Controls (SOC) 1 audits. All Neptune SaaS products are architected with Amazon best practices in mind, including the use of Virtual Private Clouds to further isolate Neptune's servers from the rest of Amazon. All network connectivity between the utility and Neptune's servers on Amazon will be protected by the use of the industry standard Transport Layer Security protocol and can be locked down to allow restricted communication to just a set of white-listed IP addresses, which are specified by the utility. We also offer the ability to set up a Virtual Private Network (VPN) connection to your site to further enhance the security of the traffic to and from the Neptune servers. Setting up a VPN requires additional hardware in your local datacenter and is recommended for utilities with dedicated IT resources.

THIRD-PARTY PENETRATION TESTING

Prior to each major release, all Neptune SaaS offerings are subjected to a rigorous third-party penetration test. Neptune ensures that the environment used for testing is configured exactly as it will be in production prior to the start of the simulated attack. This allows the test

to be an accurate gauge of how the system will respond in the event of an actual attack by a hostile third party. Our selected "pen" testers are allowed to use any tools or techniques at their disposal, including social engineering of support and development staff at Neptune. While we allow the use of automated scanning and testing tools, we ensure that this testing is heavily augmented with manual testing of the entire application as this will allow for the discovery of "zero-day" vulnerabilities that automated testing alone would likely not find. The penetration tests are executed as both an authenticated and non-authenticated user. This helps us determine if there are vulnerabilities that may allow for a privilege escalation where a legitimate user may be able to gain access to parts of the system that they should not be able to use.

Any vulnerabilities that are uncovered during the penetration test are immediately mitigated and retested to ensure that the fix not only solved the issue, but did so without introducing any new vulnerabilities. This testing is repeated until all known vulnerabilities are eliminated. While no provider of software can guarantee a solution is 100 percent secure against hacking, at the end of this process, we are able to release a product that we feel confident will withstand a sophisticated attack and help keep your data, customers, and utility safe.

MAKING SECURITY CONFIGURATION AND MAINTENANCE SIMPLE

The best security protections mean nothing if they are not properly implemented or followed, so Neptune strives to implement best-in-breed security while keeping it simple to use and maintain. We do not require any special configuration to use any of our security features. Our base controls, including encryption, are enabled by default and configured as soon as you install our system.

The final piece of the security puzzle is the people responsible for building and maintaining the systems that Neptune provides. We have created a "security first" environment where everybody shares in identifying risks and what should be done to help prevent them. This allows us to rely on subject matter experts across our company, leveraging expertise from the entire security community, to ensure that every possible point of risk, from the meter to the back-end host system, is considered as a part of our security posture. From this, we are able to build a system that is secure, rather than products that are secure on their own but may have weaknesses where they interface with one another.

All of the work Neptune has done in securing the systems we sell has resulted in enhanced security that we feel will benefit all of our customers. We want each and every system we sell to be safe and secure for its entire operating life. Working to help ensure that you have proper security in your utility is a partnership, and at Neptune we are working hard to be your **most valued partner**.

NEPTUNE TECHNOLOGY GROUP

#winyourday
neptunetg.com

Neptune Technology Group
1600 Alabama Highway 229
Tallassee, AL 36078
800-633-8754 f 334-283-7293