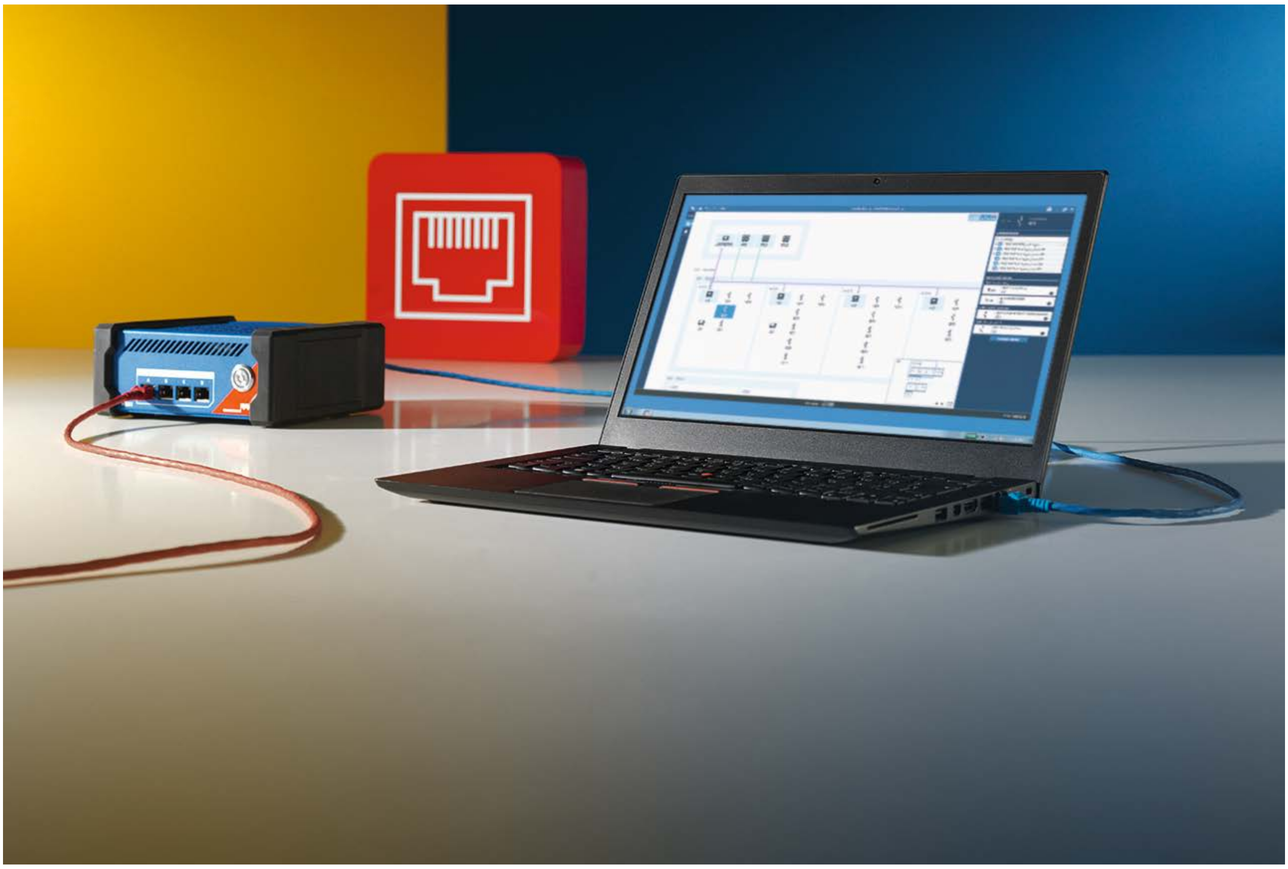
Whitepaper

Cybersecure features of the MBX1 platform



Content

1 Secure Customized Unified Extensible Firmware Interface (UEFI)

The MBX1 utilizes a customized modern UEFI which supports Secure Boot (refer to section 3). The UEFI of each MBX1 is secured with a unique password and is only accessible by OMICRON support.

2 Secure Crypto-Processor

The MBX1 is equipped with a discrete ISO/IEC 11889 compliant Trusted Platform Module (TPM2.0) chip which securely stores cryptographic certificates and supports measured boot (refer to section 3). Each TPM2.0 chip has RSA keys burned in during the production process securely seals the unique partition encryption keys used to protect the data stored on the MBX1 (refer to section 4).

3 Secure and Measured Boot

The MBX1 boot process is implemented using the secure boot and measured boot mechanisms to prevent unknown software or code from being executed on the device. Important data is encrypted and every step in the boot process verifies the signature of the next phase of the process before executing it. This ensures that only the original known and untampered software, signed with cryptographic signatures by OMICRON, is permitted to be loaded and executed by the MBX1.
Further, the secure Boot function monitors the hardware and software of the MBX1 and if it detects a change, the data in the device will not be decrypted and the MBX1 will not start.

4 Full disk encryption

All critical data on the MBX1 is encrypted and can only be decrypted by the unique MBX1 it is associated with. This means that data cannot be decrypted by third parties or OMICRON, even if the disk is transferred to another MBX1. If the data is modified on the disk through tampering, the MBX1 will detect this during the boot process and will not start.
The keys used for partition encryption are generated on the MBX1, meaning that every device has a unique set of keys. If the encryption keys of one device are compromised, this does not affect the customer data on any other device.
A new set of keys for customer data can be generated by executing a factory reset, which is only possible by physical access to the MBX1.

5 Processes execute with Least Privileges

All critical functions on the MBX1 are segregated into different processes. Each individual process runs with the minimal privileges and only the permissions necessary to perform the designated task.

6 Secure by default

The firmware and hardware of the MBX1 does not contain any default passwords or backdoors and it is only possible to enable maintenance access to the MBX1 temporarily (access is automatically closed on a restart) and with physical access to the device. The only method to allow maintenance access is to physically press the reset button on the back of the MBX1 - this activates the SSH access. Password-based SSH access is forbidden: only a challenge-response authentication mechanism requiring a cryptographic certificate is allowed and only OMICRON Service can decrypt the challenge to attain the access token to the MBX1 device.

7 Authenticated firmware upgrades

Firmware upgrades for the MBX1 are signed (SHA512) with an OMICRON certificate. This ensures the authenticity and integrity of the firmware update file. Additionally, the firmware update files are encrypted with the aes-256-cbc encryption mechanism to prevent reverse engineering. The keys for decrypting and verifying the firmware update file are securely stored on the crypto-processor (TPM2.0) chip.

8 Effective isolation of the Windows PC from the system under test.

The Windows PC (or PCs) connected to the control ports of the MBX1 and running the StationScout software only perform visualization and user interface functions with all other functionality being executed by the firmware within the MBX1. The MBX1 does not pass any data between the four substation and two control network ports. The communication between StationScout and the MBX1 is authenticated and encrypted using TLS 1.3 and StationScout only accepts connections to devices which provide the MBX1 security certificate.
The MBX1 provides both a protocol break and operating system break between the controlling PC and the substation networks.

OMICRON is an international company serving the electrical power industry with innovative testing and diagnostic solutions. The application of OMICRON products allows users to assess the condition of the primary and secondary equipment on their systems with complete confidence. Services offered in the area of consulting, commissioning, testing, diagnosis and training make the product range complete.

Customers in more than 160 countries rely on the company's ability to supply leading edge technology of excellent quality. Service centers on all continents provide a broad case of knowledge and extraordinary customer support. All of this together with our strong network of sales partners is what has made our company a market leader in the electrical power industry.

For more information, additional literature, and detailed contact information of our worldwide offices please visit our website.

www.omicronenergy.com