Leclanché
Energy Storage Solutions

MFC secure communication state

David Vermeulen 12/03/2019

TLS in NETMF 4.3

Leclanché
Energy Storage Solutions

The plan (then)

NETMF SSL support as described when we started.

SSL allows you to secure the communications between your device and a remote server. Currently only SSL2, SSL3, and TLS1.0 are supported. Your NETMF device must have the proper time set for SSL to function.
Unlike your PC, NETMF devices do not maintain a database of root certificates which are used to verify a remote server is who it says it is. As a result, you must manually include the root certificate for the site you are connecting to in your project.

The reality (now)

Implementation was done but TLS1.0 is not considered secure anymore.
TLS implementation has a memory leak that will not be fixed.
The NETMF SslStream we need to use for ftps is not stable.

Conclusion

Current NETMF TLS networking support can not be used for secure communication. (and a 4.4 fix will never be released)

Other options to transfer data in a secure way.

Leclanché
Energy Storage Solutions

- Gateway device (for AGV this could be service tool)
- Secure External modem that is handling the authentication.
- Port to TinyCLR 1.X when released. (TinyCLR is the successor to NETMF)

(We've shipped TinyCLR 1.0 (Dec 2018) and have begun to work on the next version. We will continue to evaluate stability and may issue some bug-fix only releases like a 1.0.1. The bulk of our effort is going towards the next major release where we plan to investigate commercial features like In-Field Update, USB Host and USB Client and networking -- specifically a built-in networking and TLS stack with drivers for our Ethernet PHYs and perhaps also some WiFi modules. Previews for these features will start landing over the next few months.)

https://docs.ghielectronics.com/software/tinyclr/roadmap.html

Leclanché

Energy Storage Solutions