Secure M2M in cyber-physical systems
dependability through DTLS

Motivation

• In secure cyber-physical systems YOU can help to secure a real cyber-physical system.

• Communication to alpine locations via wide area networks often suffers low-bandwidth and or transmission quality. DTLS gives applications more control than TLS/TCP to adapt to such situations.

• Don’t let nature’s heart bleed, or the poodle bite you, see your solution in real life, if YOU are successful.

We offer

• YOU gain experience in secure IoT technology such as DTLS.

• Get a complete development environment with IDE set-up on a Laptop/PC, compiler and linker incl. necessary adjustments to the hardware for the Project. Plus a running debug-able „starting-project“ on the hardware.

Project description

• Cross-compile GnuTLS (depends on nettle and gmp) for the target platform.

• Bind to ARTX-166 Transport Layer, make tests with various connection parameters.

• Compare with wolfSSL, botan, polarSSL, uSSL (in case we get eval. versions CMX-Inet-Plus, MatrixSSL or suggest a stack).

Deliverables

• Running DTLS/IPSec Stack.

• Project files (.zip, cleaned)
• Documentation (inline)
• Readme (getting started)
• Presentation (10 .ppt slides)

Project schedule

• Start Immediately
• Month 1 Exploring ARTX-166 GnuTLS development,
• Month 3 Testing, final deliverables

Bachelor Project

Studies: ☑ INF ☑ SEW ☑ TEL

Prerequisites

GIT / some C programming / make & config

Advisor / contact

Konrad.Lanz@iaik.tugraz.at