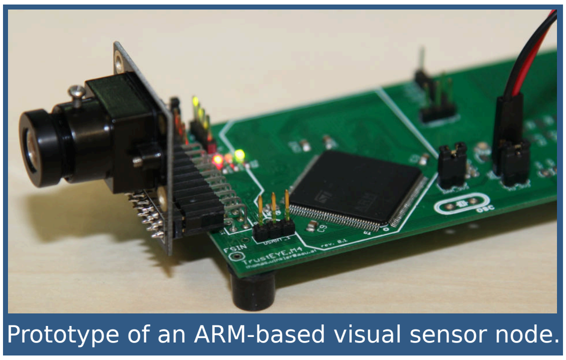
TrustEYE
Trustworthy Sensing and Cooperation in Visual Sensor Networks

The Pervasive Computing Group is looking for a student from the field of Information Technology or Computer Science for a **research project** or a **Bachelor / Master thesis** entitled:

Implementation of Security-Enhanced Bootloader for an ARM-based Microcontroller Systems

This work will be performed as part of the TrustEYE research project. Background information about the TrustEYE project and its goals can be found at http://trusteye.aau.at


Prototype of an ARM-based visual sensor node.

Work Description

Microcontrollers are programmed typically via dedicated interfaces such as **JTAG** or **SWD**. An alternative is the implementation of a small **initial bootloader** which resides in the flash of the microcontroller and which accepts the download of new program code, e.g., via a serial interface. This serial programming capability makes microcontroller-based systems a lot more convenient and accessible to developers. However, the software update procedure itself raises a number of **security concerns**. A new firmware image should only be accepted and flashed by the bootloader if a number of pre-conditions (e.g., **integrity, authenticity, freshness**) are satisfied. The goal of this work is to collect and define the required features for a security-enhanced bootloader. A review of related literature as well as a classification of existing (and openly available) bootloaders are important steps of this work. Based on this classification and the requirements from the initial project phase, either an existing bootloader should be extended to meet the requirements of the project or a new, custom bootloader should be implemented. The availability of a **Trusted Platform Module** (TPM) on the microcontroller system opens additional possibilities to implement a secure boot procedure.

Required Skills:
- C/C++

Desired Skills:
- Basic experience with microcontrollers
- Knowledge of basic security concepts
- Linux (host system)

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT I WIEN GRAZ

Contact:

Thomas Winkler
Institute of Networked and Embedded Systems
Alpen-Adria-Universitaet
Klagenfurt, Austria
P: +43 463-2700-3672
E: thomas.winkler@aau.at
W: http://trusteye.aau.at

Partners & Sponsors:

NUS National University of Singapore
KWF Kärntner Wirtschaftsförderungs Fonds
FWF Der Wissenschaftsfonds.
Investition in Ihre Zukunft
EFRE Europäischer Fonds für regionale Entwicklung
kofinanziert von der Europäischen Union