Embedded Systems Projects 2020/2021

(v8 - last update 25/01/2021)

BT-enhanced Arduino (default project for integrated project with Wireless Communications course) [contact marco.santic@univaq.it and piergiuseppe.dimarco@univaq.it]

The goal of the project is to analyze the App Immuni "ecosystem" from several points of view and to perform some experimental activities to support such analyses.

The elements to be analyzed are:

- The App Immuni and its interaction with the Exposure Notification Service API
- The implementation of the Exposure Notification Service API
- The interaction of the Exposure Notification Service with the HW/SW platform (with focus on the OS and the BT chipset)
- Available BT chipsets for the Arduino kit used in the course

The analyses to be performed are related to:

- Security (privacy and vulnerabilities)
- Energy consumption
- Reliability (correctness and accuracy)

Different groups of students will focus on different elements/analyses combinations. After a preliminary theoretical work, some experimental activities will be jointly defined.

Some References

App Immuni

1. Github Immuni: Repository with documentation and source code

Exposure Notification Service

1. Bluetooth Exposure Notification Specification: brief definition of common implementation requirements for Android-based and iOS-based devices.
2. Google Exposure Notification API: API for Android-based device
3. Apple Exposure Notification API: API for iOS-based device

Publications related to performance

1. Hernández-Orallo et al.: Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19. IEEE Access 2020
2. Leith, D. et al: Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection. ACM SIGCOMM Computer Communication Review 2020.
3. Hatke,et al,: Using Bluetooth Low Energy (BLE) Signal Strength Estimation to Facilitate Contact Tracing for COVID-19. 2020. Preprint.

Publications related to security

1. Azad, M.A et Al,: A First Look at Privacy Analysis of COVID-19 Contact Tracing Mobile Applications. IEEE Internet of Things Journal 2020, Early Access
2. Garg, L.et Al: Anonymity Preserving IoT-Based COVID-19 and Other Infectious Disease Contact Tracing Model. IEEE Access 2020.

Examples of BT modules for Arduino

1. HM-10 (BLE 4.0): https://www.amazon.it/dp/B06WGZB2N4
2. HM-19 (BLE 5.0): https://www.amazon.it/dp/B07MBLVHH8/

Dynamic Partial Reconfiguration (DPR) [contact giacomo.valente@univaq.it]

The DPR (also called *Dynamic Function Exchange*) is a process offered by *Field Programmable Gate Arrays* (FPGAs) to change at runtime the hardware architecture implemented with the FPGA. This enforces the capability to self-adapt in response to external factors.

DPR.1

The goal of this project is, through the usage of DPR, to organize the self-adaptation of an aerospace embedded system that executes a Sobel image detection algorithm. The self-adaptation happens in response to an external disturbance (experimentally triggered by a push-button).

DPR.2

The goal of this project is to manage DPR using a real-time operating system, namely Free-RTOS. In particular, a context-switch shall be performed in response to an external factor, in order to self-adapt an embedded system using the DPR.

Monitoring Systems (MS) [contact giacomo.valente@univaq.it]

During the design of an embedded system with limited resources, there is often the need to characterize what happens inside the system at runtime, in order to optimize design choices. The simulation is not always a viable solution but there is the need to build a system with embedded monitors that allow to understand what is happening.

MS.1

The goal of this project is to maximize the performance of an embedded system by introducing a MS. The MS is able to observe memory accesses, in order to provide feedbacks that can be exploited by modifying the application source code.

MS.2

The goal of this project is to verify the correct behavior of an application executed directly on the final target (runtime verification). To do that, a MS able to perform the *tracing* (i.e., to keep a timestamped track of what is doing the system) is adopted.

Wireless Sensor Networks [contact walter.tiberti@univaq.it]

WSN.1: Cryptography on Embedded Systems/WSN

Implementation of Poly1305 Message Authentication Code Function on WSN node. In this project, the student has to develop an optimized implementation of the Poly1305 MAC function for WSN using the C language and the TinyOS framework. The implementation has also to be tested by developing the required WSN applications and a scenario involving WSN node communication and message authentication.
References:
https://tools.ietf.org/html/rfc7539
https://cr.yp.to/mac.html

WSN.2: Intrusion Detection Systems for WSN

Development of a set of attacks targeting WSN
In this project, the student has to develop a set of networking/application-level attacks targeting WSN nodes. Those attacks will be used to evaluate the security of the WSN and to evaluate a WSN Intrusion Detection System and its the ability to detect such attacks. Example attacks could be:
- Jamming attacks / DoS (also DdoS) / DeAuth ...
- Man-in-the-middle / Sybil attacks
- Wormhole / Sinkhole
- Application logic vulnerabilities (e.g. Buffer overflows)

Development of a set of *reactions* to WSN attacks
In this project, the student has to propose and implements reactions strategies and mechanisms in a WSN under attacks. Given the notification of a in-progress attack, those mechanisms should do everithing to prevent the attacks to further damage the WSN by 1) identifying the position of the attacking nodes or other valuable information about the attack; 2) limit the attack surface or, when possible, isolate the attacking nodes

WSN.3: Energy Measurement for WSN

Energy Measurement for WSN nodes using a current-measurement board
In this project, the student will use a external board featuring a configurable DC current-measurement IC to measure the current, power and energy consumed by real WSN when running a set of meaningful applications (i.e., benchmarks). In particular, the objective is to 1) learn of to use the external board 2) develop a set of benchmarks and 3) measure the energy consumed by different WSN nodes when running the benchmarks

Analysis and Improvement of Omnet++ Energy Consumption models for IEEE 802.15.4 networks
In this project, the student has to analyse the state-of-the-art of the energy models available in the Omnet++ simulator and in its INET library, use them in a set of meaningful scenarios, eventually improving them to better estimate the real energy consumption of WSN nodes.

WSN.4 TinyGIS – GIS on top of a TinyOS-based distributed DBMS

Development of a set of GIS *spatial operators* to extend an existing DBMS solution for TinyOS-based WSN
In this project, the student has to analyse the *TinyDB* DBMS and extend it by implementing a set of classical GIS spatial operators.
References:
http://telegraph.cs.berkeley.edu/tinydb/index.htm
http://cs.uccs.edu/~cs526/mote/tinyos/tutorial/tinydb.html

WSN.5 Application Security for Embedded Systems and WSN

Vulnerability analysis and exploitation of common libc implementations for Embedded Systems

In this project, the student has to analyse (i.e., source code analysis and reverse-engineering) the implementation of the C-library available in the SDK of common Embedded Systems platform. In particular, the focus is on the following platforms:
- Arduino / AVR micro-controllers and the *avr-libc* implementation
- MSP430, both *msp430-glibc* and *msp430-elf-glibc*

WSN.6
LabSmiling: remote testbed for WSN

RTOSs and HPVs [contact vittoriano.muttillo@univaq.it]

RTOS.1
Analysis and experimentation of MuteKH
Main links (main results from Google search):
https://www.mutekh.org/
https://www-soc.lip6.fr/trac/mutekh
https://www.soclib.fr/appliance/docs/mutekh-vfs/index.html
https://www.openhub.net/p/mutekh
http://www.comelec.telecom-paristech.fr/uploads/tx_dbcomelec/20130110_01.pdf
http://www.soclib.fr/trac/dev/wiki/Tools/Mutekh

RTOS.2
Analysis and experimentation of NuttX
https://nuttx.apache.org/

SW Development for DSP [contact paolo.giammatteo@univaq.it]

DSP.1
The project proposal focuses on the development of a SW implementation of an agent-method synchronization methodology. The implementation will be developed on DSP system, two or more in network. The device proposed is a Texas Instruments DSP. The aim is to reach the synchronization of a variable managed by each DSP through a consensus algorithm.

SW Development for GPGPU [contact paolo.giammatteo@univaq.it]

ESL HW/SW Co-Design [contact luigi.pomante@univaq.it]

ESL.1
HEPSYCODE-based (https://www.hepsycode.com/) DSE for the Digital Camera case study

ESL.2
System-Level DSE for Energy/Power

ESL.3
System-Level DSE for Approximate Computing

ESL.4
HEPSYCODE-based Multi-MOC Simulation

ESL.5
Experimentation of system-level design flows

ESL.6
Customization of HEPSYCODE for FPGA

ESL.7
Customization of HEPSYCODE for ZYNQ-like SoPC

ESL.8
Analysis and experimentation of SystemC TLM.

ESL.9
Analysis and experimentation of the IP-XACT standard and comparison with UML/MARTE

ESL.10
Analysis and experimentation of SoClib
http://www.soclib.fr/trac/dev

Miscellaneous (M) [contact luigi.pomante@univaq.it]

M.1
Re-engineering of the 8051 HomeLab

M.2
Re-engineering of the Digital Camera Case Study

M.3
SW Development for the RC-64 Many-Core Processor

M.4
Development of Machine Learning Applications with the Xilinx VERSAL SoC