LATVIJAS UNIVERSITATE
ANNO 1919

Specseminārs

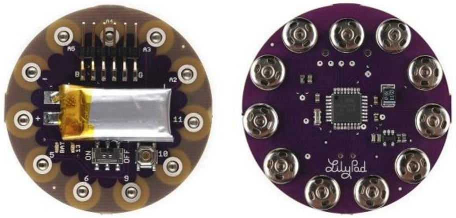
Kiberfizikālās sistēmas, tai skaitā sensori, iegultas iekārtas, to programmēšana un robotika

20.11.2014

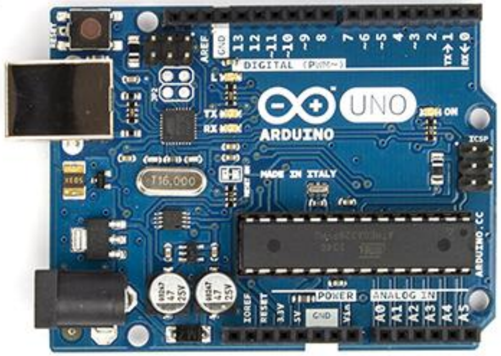
Artis Mednis
Leo Seļāvo

Arduino ekspresaptauja

- Cik no Jums ir pamēģinājuši Arduino vismaz “Hello, world!” līmenī?



- Cik no Jums šobrīd veido projektu (vai plāno veidot projektu) uz Arduino bāzes?



- Vai ir kāds, kas gribētu taisīt kaut ko nopietnāku (piemēram – bakalaura darbu) uz Intel Galileo bāzes?

Klonētās sistēmas

- Oficiālie jeb Arduino [kaut-kas]
  - **Esošie** (piemērs – Arduino Uno)
  - **Bijušie** (piemērs – Arduino Duemilanove)
- Arduino savietojamie jeb [kaut-kas]duino
  - Savietojamība **pēc HW un SW** (kloni, piemērs - Freeduino)
  - Savietojamība **tikai pēc SW** (atšķiras HW formfaktors, piemērs - Boarduino)
  - Savietojamība **tikai pēc HW paplašinājumiem** (atšķiras gan HW, gan SW, bet var izmantot oriģinājos vai klonētos papildmoduļus, piemērs - Netduino)

Nedaudz par praktisko pieredzi ar Arduino izmantošanu konkrēta projekta realizācijai…

ELEKTRONIKAS UN DATORZINĀTŅU INSTITŪTS
INSTITUTE OF ELECTRONICS AND COMPUTER SCIENCE

RFID Communication: How Well Protected Against Reverse Engineering?

Artis Mednis[13], and Reinholds Zviedris[23]

[1] Cyber-Physical Systems Laboratory, [2] Digital Signal Processing Laboratory
Institute of Electronics and Computer Science,
14 Dzerbenes Str, Riga, LV 1006, Latvia

[3] Faculty of Computing, University of Latvia,
19 Raina Blvd., Riga, LV 1586, Latvia
{firstname.lastname}@edi.lv

ESF
EIROPAS SOCIĀLAIS FONDS

EIROPAS SAVIENĪBA

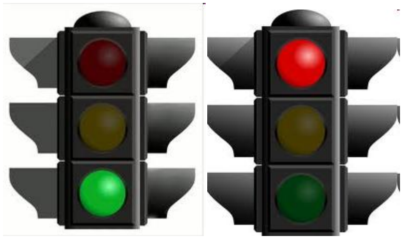
LATVIJAS UNIVERSITATE
ANNO 1919

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Research area and motivation I

- Typical RFID system:
  - one or several RFID **tags** (active or passive)
  - one or several RFID **readers**
  - **data processing** subsystem

- Typical RFID applications:
  - **identification** and **tracking** of several objects and subjects
  - management of the **access rights**
  - **additional functionality** for common person documents



Research area and motivation II

- RFID tags categorized by security:
  - tags for **logistical** applications – no or little routine for security
  - tags for **consumer** applications - with security capability
  - tags for **vertical** applications – with security tailored for specific business processes

- RFID system investigated during this research:
  - intended for measurement of the **timing** during sporting events
  - commercially **available** and relatively **wide used**
  - belongs to the **third** above mentioned category

State of the art

- Hard to ensure secure communication in low-cost RFID systems:
  - hardware and software **resources** are constrained
  - strong **cryptographic** solutions are not possible
  - lightweight algorithms and protocols can be **broken** by a powerful attacker

- Attack methods (and their prevention):
  - **eavesdropping** or **skimming** of forward and backward channels
  - tag **cloning** (symmetric-key cryptography and security protocols based on Physical Unclonable Function (PUF))
  - **physical** attacks (making tags more secure against tampering)
  - **relay** and **replay** attacks (sequence numbers and clock synchronization)
  - **deactivation** of the tag using corresponding command (PIN code)

Requirements

- Reverse engineering of the specific RFID system should be performed using **relatively simple reverse engineering techniques**. Usage of specific software tools as well as pool of computing devices is not intended.

- The **black box approach** should be used for exploration of the RFID communication protocol physical and logical layers. Dismantling or physically damaging hardware items as well as social engineering for acquiring of classified information are not intended.

- Additional hardware and software necessary for reverse engineering activities should be **freely available**, **relatively inexpensive** and characterized by steep learning curve.

- Communication of specific RFID system should be considered as insufficiently protected against reverse engineering if there is a possibility to **simulate a non-existing RFID tag with certain self selected ID number** using above mentioned relatively simple tools and methods.

Approach

- Investigation of the **physical layer** of RFID system communication protocol.

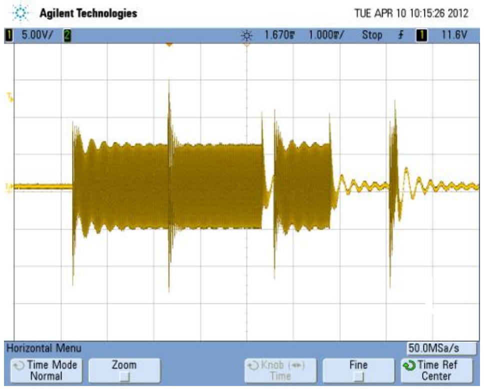
- Development of the **toolset** consisting of off-the-shelf hardware and software with the aim to simulate corresponding RFID system components.

- Investigation of the **logical layer** of RFID system communication protocol.

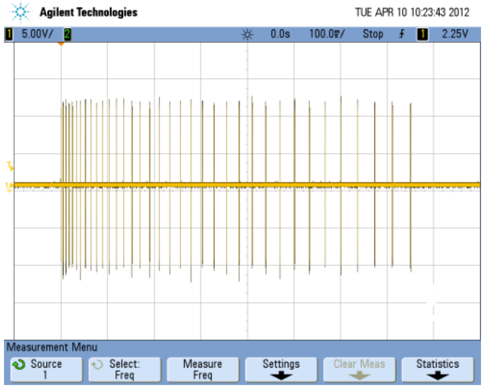
- Development of the **method** to simulate a non-existing RFID tag with certain self selected ID number.

Communication protocol physical layer

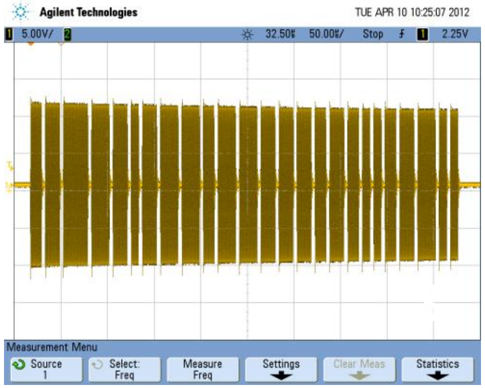
- RFID reader **calling** message (1):
  - sequence of OOK modulated 125 kHz oscillations
  - 80 times per second



- RFID tag **entire response** message (2):
  - 36 sequential single response messages
  - time interval between sequential messages incrementing from 4 ms to 39 ms

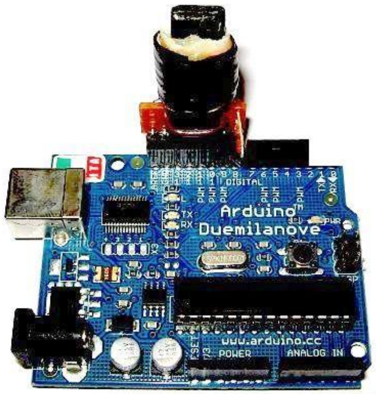


- RFID tag **single response** message (3):
  - sequence of OOK modulated 3 MHz oscillations
  - 25 ON items with the length from 9 to 28 μs
  - 24 OFF items with a fixed length of 3 μs



Hardware and software

- Open source electronics prototyping platform **Arduino** and its board - Arduino Duemilanove



- Simulated RFID **reader** (1):
  - Arduino + circuit consisting of a **magnetic antenna** in series with appropriate resistor
  - software not only for OOK modulation but also for generation of the main oscillations

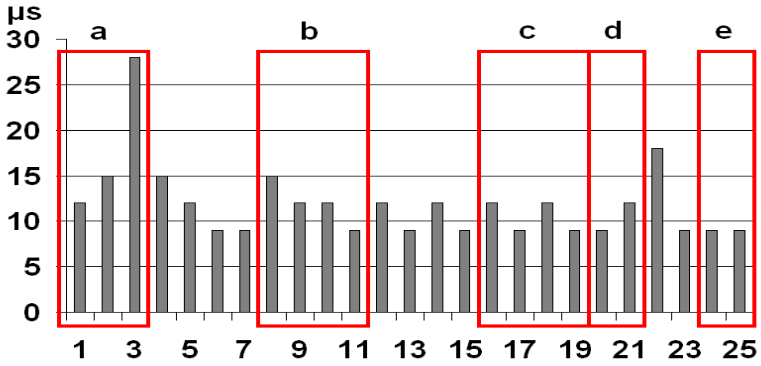
- Simulated RFID **tag** (2):
  - Arduino + circuit consisting of **3 MHz oscillator**
  - software only for OOK modulation

Communication protocol logical layer I

- **Each** single response message contains **all** information transmitted from RFID tag to RFID reader

- Potential **meaning** of the different message parts:
  - first 3 ON items as preamble part (a)
  - last 2 ON items as postamble part (e)

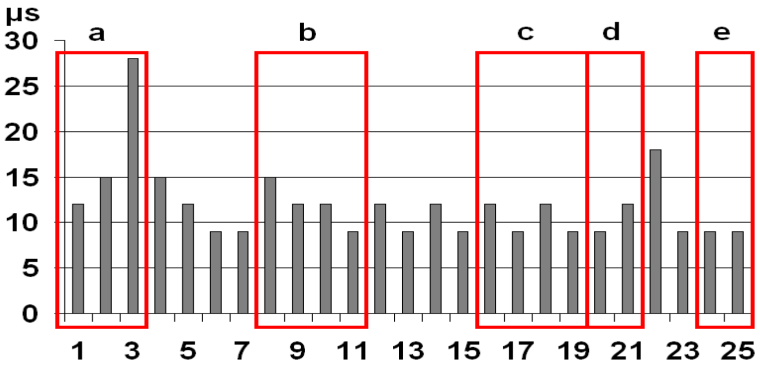
- ON items lengths, except the #3 which length was 28 µs, are strictly one from the following list:
  - 9 µs
  - 12 µs
  - 15 µs
  - 18 µs



- Could it be the **quaternary** numeral system? ...

Communication protocol logical layer II

- Clarification:
  - both **original ID numbers** consisting of 5 decimal digits were converted to **quaternary numeral system**
  - both **obtained ID numbers** consisting of 9 quaternary digits were compared to corresponding **single response messages**



- Results:
  - 9 μs -> 0, 12 μs -> 1, 15 μs -> 2, 18 μs -> 3
  - ON items 8..11 -> quaternary ID digits 6..9 (b)
  - ON items 16..19 -> quaternary ID digits 2..5 (c)
  - *ON items 20..21 -> quaternary ID digit 1 with leading zero*
  - 10 another ON items - internal battery level and **checksum**

Simulation of non-existing RFID tag I

- **10 ON items** that could be **considered** as **checksum**

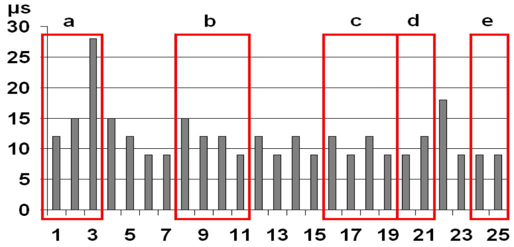
- Algorithm using brute force attack principles :
  - all 1 048 576 possible single response messages for particular ID number are transmitted to the RFID reader in **sequential** order
  - each individual single response message is **repeated** 12 times
  - time **intervals** between subsequent transmitted single response messages are 4 ms long

- There are at least **4 possibilities** for RFID reader to detect valid single response message

- Total time of the transmission is about 15.6 hours... **Too much...**

Simulation of non-existing RFID tag II

- Quaternary digits representing ID number digits are grouped in 3 sequences:
  - 2 sequences containing 4 digits (b and c)
  - one sequence containing 2 digits (d)



- Quaternary digits representing checksum (and the charge level of the internal battery) are grouped identically

- Most significant ID number digits are stored in the shortest sequence and it is supposed that this short sequence in most cases is invariable therefore potentially not so significant for checksum calculation

- Shortest sequence of the checksum (and the charge level of the internal battery) allows transmitting 16 different levels of charge level and similarly to shortest sequence of the ID number digits, in this case could be relatively invariable

- What about **just 8 ON items** for checksum?

Evaluation

- Following set of the activities were performed:
  - selection of a non-existing ID number which differed from one of the real ID numbers by two quaternary digits
  - development of the Arduino software for subsequent transmission of 65 536 possible single response messages 12 times
  - test with developed hardware and software with the aim to determine a valid single response message containing self selected ID number

- Several features such as automatic detection of a valid single response message and extraction of corresponding checksum were not implemented in the software but performed by test operator manually

- Successful determination of a valid checksum for the particular self selected ID number took **just about 1.2 hours**

Conclusions

- It is possible to make **successful** reverse engineering of particular RFID communication using relative **simple** tools and methods

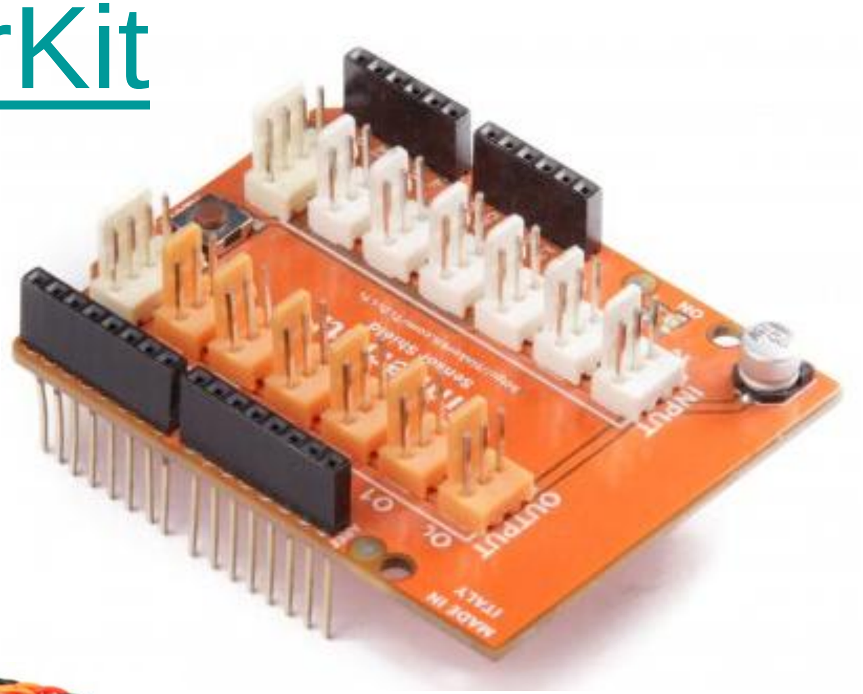
- The performance of developed reverse engineering method could be **improved** using **automatization** of manually performed actions as well as **optimization** of transmitting sequence

- The future work includes experiments in generation of RFID communication message with the aim to **decrease** the time for acquiring of a valid message exchange as well as further exploration of the communication protocol’s **logical** layer

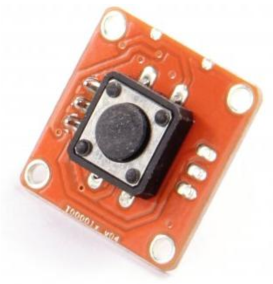
Thank You! Questions?

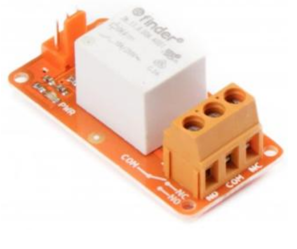
Un tagad atpakaļ pie mūsu pamata tēmas ☺

TinkerKit



- Sensor Shields
- Wires
  - 3pin/4pin
  - 20/50/100cm
- Modules
  - sensors
  - actuators





Praktiskais darbs

Arduino TinkerKit

- Izpētīt komplektos ietilpstošos **sensorus** un **aktuatorus**
- Izpētīt bibliotēkā ietilpstošos **programmatūras paraugus**
- Uz izpētīto resursu bāzes realizēt savu **sense-analyze-execute** risinājumu
- Nodemonstrēt savu risinājumu, pastāstot, kas **ņemts par pamatu**, un kas **pielikts klāt no sevis**