Hardware password manager based on biometric authentication

Keywords: Biometric Authentication, Security, Cyber-Physical systems; Mechatronic Devices

Password manager and biometric authentication Issues

From the multitude of problems regarding the security of distributed communication systems, composed of mobile and fixed networks, the present work focuses on some modern, possible approaches and corresponding, efficient solutions, applicable for encryption and authentication purposes.

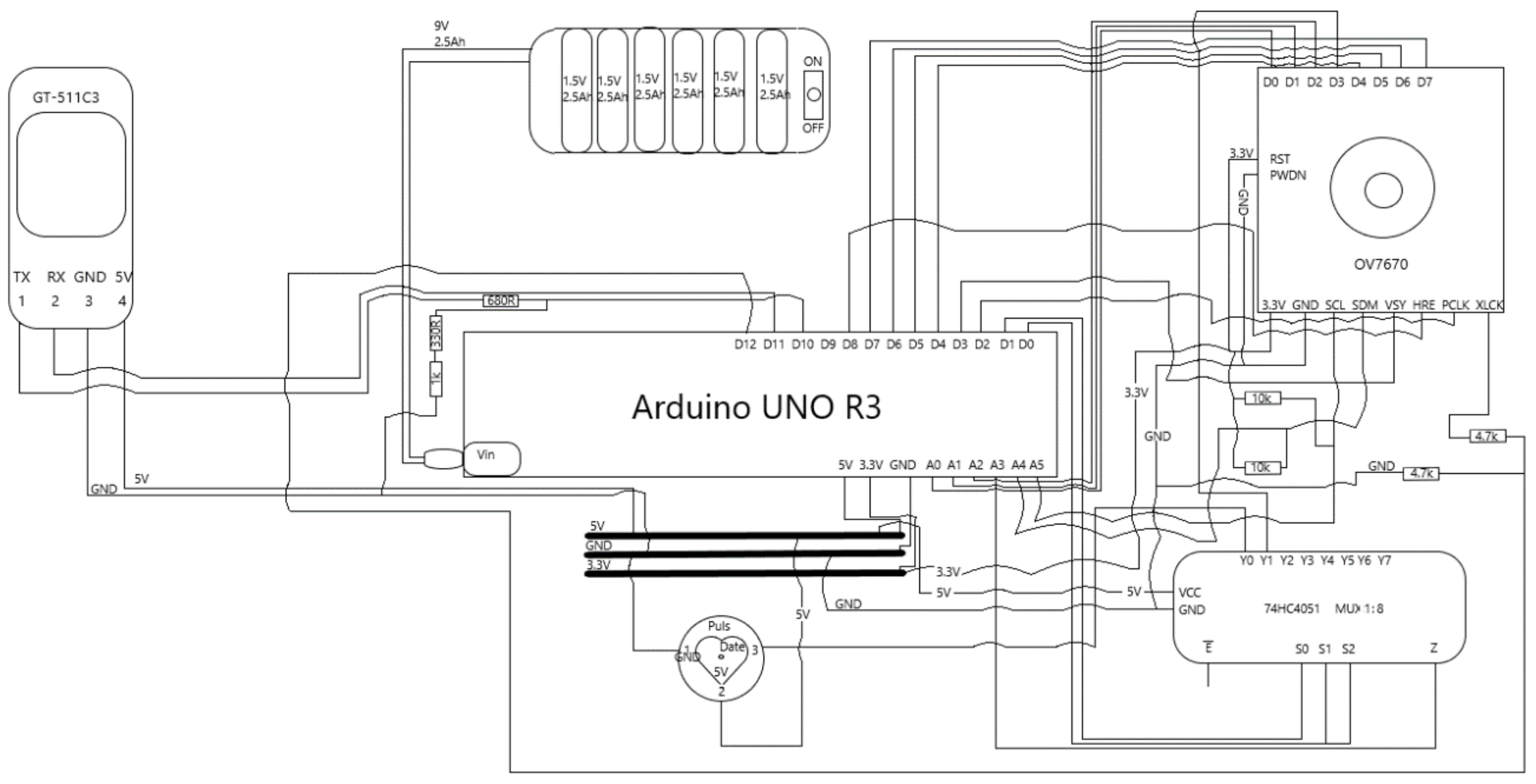
The processed fingerprint of the user, to which the iris and pulse are associated and used for the generation of a symmetric key is having a short life span.

This method transforms an apparent disadvantage of the fingerprint sample (two successive samples of the same fingerprint are given never the same image) in an important advantage, useful from the point of view of confidentiality. This way the premises of a short life span, for each communication session are fulfilled.

The method is suitable for user authentication on websites using stored encrypted password.

Design and implementation

- 3DPassManager is a wearable device that uses fingerprint and iris, measures heartbeat and uses it as a unique biometric authentication. The password is generated based on fingerprint details and is valid for a small-time interval.
- When initializing the authentication process, the fingerprint and iris are used to ensure that the person using the device is the rightful owner, and the pulse is used to verify if static images, previously acquired, are not used.
- Once the person is authenticated, the rest of the stored passwords in the device are accessible.
- The fingerprint is stored in a 1024-bit long key. Once the device is authenticated the passwords are available trough an extension installed on the web browser.
- Each stored password is encrypted, and the user's fingerprint is the key.
- The device is the size of a cigarette pack and communicates with the PC trough BT



3DPasManager - Hardware components

Simulation and Verification of Results

Several performance tests were performed.

Temporal performances of the device for the main activities

Activity	Tmin	Tmax
Connection and initialization of fingerprint sensor	1s	1.2s
Connection and initialization of iris sensor	1.1s	1.3s
Connection and initialization of pulse sensor	0.8s	1.1s
Testing the fingerprint sensor connection	650ms	700ms
Testing the iris sensor connection	680ms	690ms
Testing the pulse sensor connection	670ms	680ms
Fingerprint reading	761ms	780ms
Iris reading	690ms	782ms
Pulse reading	680ms	702ms

Temporal performances for the communication between 3DPassManager and a PC/laptop

Activity	Tmin	Tmax
Authentication	1s	2s
Record a new subject	3.1s	8.3s
User checking	3 s	8s
User identification	0.8s	1.3s
Searching for Bluetooth devices	14.6s	20s
Connecting Bluetooth devices	1.8s	3.1s
Authentication	1s	2s
Record a new subject	3.1s	8.3s
QR code scan	1s	1.4s

Authors:

Camelia Avram[1], Jose Machado[2] and Adina Astilean[1]

[1] **TUCN, Cluj Napoca, Romania,**

[2] **U Minho DME, Portugal**

MINISTRY OF EDUCATION
TECHNICAL UNIVERSITY
OF CLUJ-NAPOCA, ROMANIA