Alexis Quesada-Arencibia
José Carlos Rodríguez
Roberto Moreno-Díaz
Gabriele Salvatore de Blasio
Carmelo Rubén García (Eds.)

EUROCAST 2022

Computer Aided Systems Theory

EXTENDED ABSTRACTS

18th International Conference on Computer Aided Systems Theory
Las Palmas de Gran Canaria, Spain, February 2022

Eighteenth International Conference on
COMPUTER AIDED SYSTEMS THEORY

EUROCAST 2022

Edited by

Alexis Quesada-Arencibia
José Carlos Rodríguez-Rodríguez
Roberto Moreno-Díaz
Gabriele Salvatore de Blasio
Carmelo Rubén García

ISBN: 978-84-09-38381-8
REGISTRO: 2022011735

Lightweight Cryptography for BLE Tracking ⋆

D. Cruz-Rodríguez[1], C. Hernández Goya[1], and R. Aguasca-Colomo[2]

[1] Departamento de Ingeniería Informática y de Sistemas
Universidad de La Laguna. SPAIN
[2] Instituto Universitario de Sistemas Inteligentes y Aplicaciones Numéricas en Ingeniería,
University of Las Palmas de Gran Canaria, 35017 Gran Canaria, Spain
{alu0101105802@ull.edu.es, mchgoya@ull.edu.es,
ricardo.aguasca@ulpgc.es

1 Introduction

In this work, a service to track mobile devices is presented. The service integrates information protection mechanisms to guarantee confidentiality and integrity.

2 Description

The service consists of an Android application and a backend, hosted in the cloud, which deploys a web server. It follows a microservice structure over containers allowing a simple management and distribution. The Android application implements two modes of operation: the client mode, intended for the devices that are tracked and, the tracker mode executed by a smartphone on board a Remotely Piloted Aircraft (RPA) (see figure 1). The application running on the clients uses the Bluetooth Low Energy (BLE) beacon mode to transmit information related to their positioning and trajectory (latitude, longitude, height, bearing and speed) along with a randomly generated Unique IDentifier for each client device. The on-board smartphone will allow to transmit the collected data, using 4G/5G communications, to a web server to be represented and exploited. This system can be deployed in different scenarios to respond to multiple situations such as supervision and control of risk situations in crowded areas, tracking and tracing people in isolated environments.

The beacon communication mode does not require prior pairing between parties. However, given the restrictions defined in the communication frames, an adhoc encoding scheme was defined. The specific protocol used by client devices is Eddystone, defined by Google as a standard for Bluetooth beacons.

The data mining module in the backend will allow us to represent the current position of each client, as well as their track record over time. Adding bearing and speed information would facilitate new module development using AI for event monitoring to detect possible dangerous or risky situations.

⋆ Research supported by the Spanish Ministry of Science, Innovation y Universities (MCIU), the State Research Agency (AEI) and the European Regional Development Fund (ERDF) under project RTI2018-097263-B-I00.

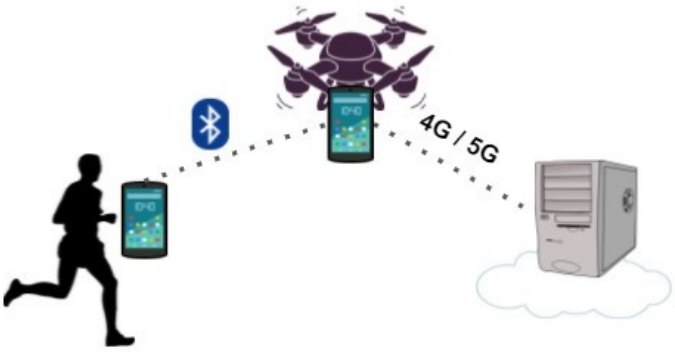

Figure 1. Esquema global del sistema.

3 Security: Integrity and confidentiality

The confidentiality and integrity services have been implemented using cryptographic primitives belonging to Lightweight Cryptography. In the implementation we have chosen to use Chaskey [4] as the Message Authentication Code (MAC) generator and ChaCha20 as the encryption scheme. In this way an authenticated encryption [3] scheme has been generated using the Encrypt-then-MAC approach.

Chaskey is included as part of the ISO/IEC 29192-6:2019 [1] standard and is defined as a permutation-based MAC algorithm using the Addition-Rotation-XOR (ARX) design methodology. The use of the ARX approach together with the reduced length of the generated codes (they can have a minimum length of 64 bits) make it suitable for the system designed in this work.

Chacha20 [2] is a stream cipher, present in TLS, composed of 20 iterations that process the initial state through the quarter-round function using a key of length 256 bits. Given the constraints of the scenario deployed, an adhoc implementation of both procedures has been performed

References

1. 29192-6:2019, I.: Part 6: Message authentication codes (macs). Information technology — Lightweight cryptography pp. 1–20 (2019)
2. Bernstein, D.J., et al.: Chacha, a variant of salsa20. In: Workshop record of SASC. vol. 8, pp. 3–5 (2008)
3. Hwang, M.S., Liu, C.Y.: Authenticated encryption schemes: Current status and key issues. Int. J. Netw. Secur. **1**(2), 61–73 (2005)
4. Mouha, N.e.a.: Chaskey: An efficient mac algorithm for 32-bit microcontrollers. In: SAC 2014. pp. 306–323. Springer International Publishing (2014)