Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

Behavioural Sensor Data as Randomness Source for IoT Devices

SPEAKER **Ms DINCA Mihaela Lavinia**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 9 June 2017 (Friday)
TIME 12:30 pm - 1:00 pm
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Random numbers generators are very important for cryptography and using biometrics as a source for randomness is on ascending trend. Because of the multitude of IoT devices present in our daily lives the need for keys and sources of randomness increased. This paper assesses the feasibility of using IoT devices to gather data on human behaviour for creating randomness. This paper analyses the suitability of using bio- metric data collected from 6 smartphone sensors: accelerometer, gravity, gyroscope, linear acceleration, magnetometer, rotation, and sound. The sensor data is run through all three well-known batteries of tests: NIST, ENT and Dieharder. We demonstrate that human gait is highly predictable and shouldn't be used as a source of randomness. We also show that contrary to popular believe using data from two sensors slightly improves randomness, but it still doesn't pass all tests.

This paper will be presented at The 26th IEEE International Symposium on Industrial Electronics, 19-21 June 2017, Edinburgh, Scotland, UK.

Supervisor: Dr HANCKE Gerhard Petrus

Research Interests: Sensors; Data Confidentiality and Encryption; Biometrics

All are welcome!

In case of questions, please contact Dr HANCKE Gerhard Petrus at Tel: 3442 9341, E-mail: gp.hancke@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.