# First real-world study shows the potential of gait authentication to enhance smartphone security

December 10 2021, by Alan Williams



Professor Nathan Clarke. Credit: University of Plymouth

Real-world tests have shown that gait authentication could be a viable means of protecting smartphones and other mobile devices from cyber crime, according to new research.

A study led by the University of Plymouth asked [smartphone users](#) to go about their [daily activities](#) while motion sensors within their [mobile devices](#) captured data about their stride patterns.

The results showed the system was on average around 85% accurate in recognizing an individual's gait, with that figure rising to almost 90% when they were walking normally and fast walking.

There are currently more than 6.3 billion smartphone users around the world, using their devices to provide a wide range of services and to store sensitive and confidential information.

While [authentication](#) mechanisms—such as passwords, PINs and biometrics—exist, studies have shown the level of security and usability of such approaches varies considerably.

Writing in Computers & Security, the researchers say the study illustrates that—within an appropriate framework—[gait](#) recognition could be a viable technique for protecting individuals and their data from potential crime.

Academics from the University's Centre for Cyber Security, Communications and Network Research have been focused upon developing a range of innovative authentication mechanisms to provide more secure and usable solutions.

This study builds upon that prior work through the evaluation of a multi-algorithmic [gait recognition](#) system and is the first to apply this using real-world data.

For the research, 44 participants aged between 18 and 56 were each asked to carry a globally available smartphone device for seven to 10 days.

They were asked to place the [smartphone](#) in a belt pouch to record the sensor data captured by the device's gyroscope and accelerometer during the course of different physical activities.

Each participant generated an average of 4,000 sample activities during the course of the test, with these split into records showing normal and fast walking in addition to climbing and descending stairs.

This showed a potential error rate of 11.38% and 11.32% for normal and fast walking respectively, with the figures rising to 24.52% and 27.33% when participants were going down and upstairs respectively.

The researchers say this emphasizes the need to further advance the ability to automatically differentiate a wider set of walking activities so that a multi-algorithmic approach to identification can target specific walking characteristics.

Nathan Clarke, Professor of Cyber Security and Digital Forensics at the University of Plymouth, who has recently been made a Fellow of the Chartered Institute of Information Security, said: "As smartphones have developed, [security](#) controls have had to advance significantly. This has led to a significant rise in user authentication, where users repeatedly need to authenticate both their devices and the numerous apps they contain. Gait authentication has emerged as a non-intrusive way of capturing a necessary level of personal information, but—until now—all tests of it have taken place in a controlled environment. Gait recognition alone will not be the answer to usable and convenient authentication, but it could form a critically important tool within the cyber arsenal that could contribute towards creating a stronger awareness of a user's identity. This study demonstrates, for the first time outside of laboratory-controlled conditions, what level of performance can be achieved realistically. It is clear performance levels are impacted; however, the study has also shown that, for most users, these issues can be overcome

to an acceptable level."

**More information:** Hind Alobaidi et al, Real-world smartphone-based gait recognition, *Computers & Security* (2021).

Provided by University of Plymouth