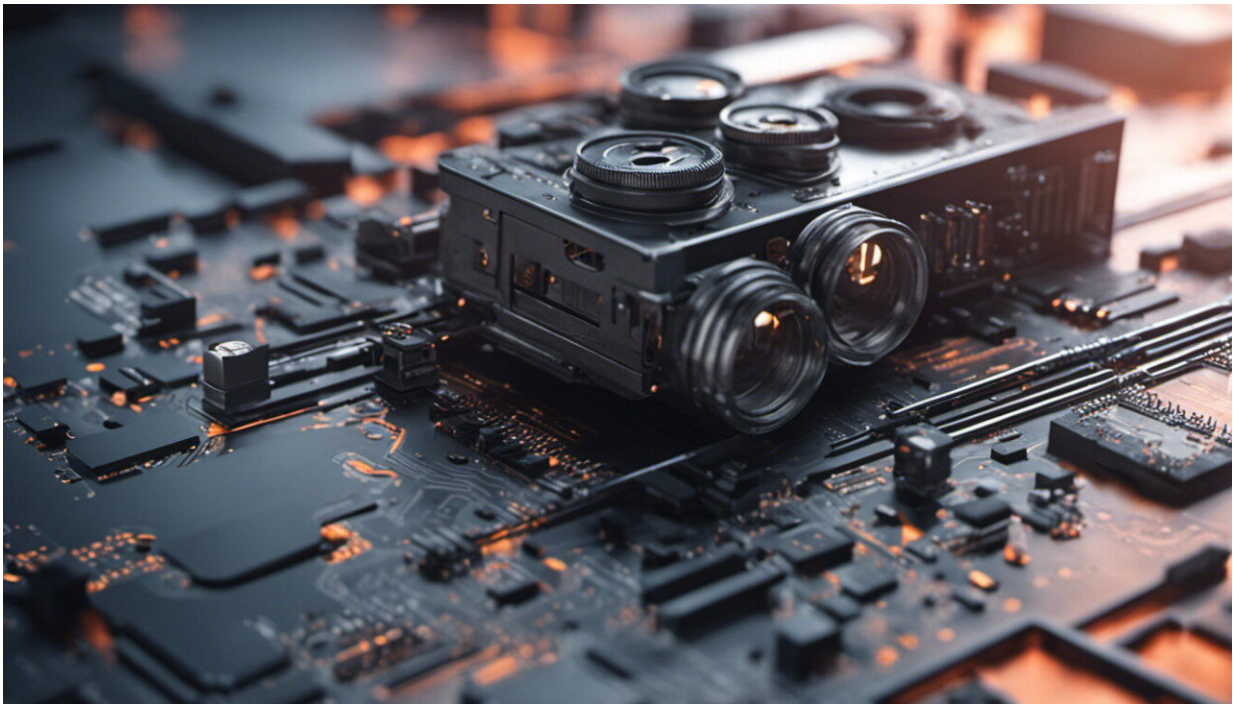


The way we walk can be used to power and secure our devices

May 24 2017, by Sara Khalifa And Dali Kaafar



Credit: AI-generated image ([disclaimer](#))

When we walk or move, we create kinetic energy in a way that is unique to each of us. Our [latest research](#) shows that it's so unique, it can be used to authenticate who we are.

Not only that, but this [kinetic energy](#) can also be used to power our

personal devices.

Power and security from the energy we create by walking is ideally suited to wearable technologies.

Wearables and [mobile devices](#) have become an integral part of our daily life. We collect and store huge amounts of personal information on those devices – accounts are synced, movements and locations recorded, and much, much more.

Many of us are tracking our health using devices such as FitBits, Apple Watches, heart rate monitors and the like. According to market research group [IDTechEX](#) the market for personable [wearable technologies](#) is expected to reach US\$150 billion (A\$200 billion) by 2026.

Data security

But [researchers have found](#) that some of these devices are vulnerable to attacks. It's also possible for [one person to connect to another's wearable tracker](#) without that person's knowledge.

A potential attacker could then connect their device to that of another user and claim that user's data as their own. For example, an attacker may be able to claim potential health [insurance discounts](#) and other benefits that are offered to people who allow insurance companies access to wearable tech data.

More worryingly, as mobile tech is being used more in healthcare monitoring of people, there's a concern that such [systems could be vulnerable to impersonation attacks](#).

Wearable and mobile devices often require some form of [user authentication](#) to address such impersonation attacks and protect the

large amounts of personal data they collect.

The password problem

Most [authentication](#) relies on pin codes and passwords to keep devices secure. But [recent research](#) shows most of us have just two passwords – with a few tweaks here and there – used across 12 separate accounts.

We're constantly being asked to choose difficult passwords, and not to write them down. Yet according to [Verizon's 2016 Data Breach Investigations Report](#), 63% of confirmed data breaches resulted from leveraging weak, default or stolen passwords.

For decades we've been trying to develop a better alternative that is neither easily compromised nor requires submitting information that only a user would know.

We're walking

One of the most promising solutions for user authentication is through recognition of our gait, or walking style, using wearable sensors such as [accelerometers](#) that measure human movements.

Because everyone has a different gait, which affects the movement of body segments differently, it can be used as a [digital fingerprint](#) to identify and authenticate a user.

The main advantages of using gait as authentication are availability and spontaneity, because walking is a daily activity.

Unlike other authentication methods, gait is non-intrusive. Our gait can be measured and tested without us even knowing. We are not required to

enter information regularly to verify that it's us. Our gait can be used continuously for authentication.

But there's a catch – sampling our movements saps power from our devices.

We are a power source

Accelerometer sampling of our movements requires power, typically in the order of a few milliwatts. This makes it challenging to adopt gait-based user authentication in wearables where power availability is limited.

Simply adding a bigger battery to a [wearable device](#) or charging more regularly are not practical solutions.

To combat this issue, there is a [strong interest in kinetic energy harvesting](#) (KEH). This translates our motion into electrical energy that can be used as a trickle charge, improving battery life on wearable devices.

Some wearable KEH products are already appearing in the market. [AMPY](#) released the world's first wearable motion-charger which can transform a user's kinetic energy into battery power. Similarly, [SolePower](#) produces smart boots that use a user's steps to power embedded lights, sensors and GPS.

With these rapid developments, KEH is likely to be built in to future wearable and mobile devices to augment or substitute batteries.

Unique kinetic energy harvesting

By examining the output voltages of KEH, [we found](#) that each of us also

has unique energy patterns when performing different activities.

KEH therefore represents not only a power source but also another form of authentication.

The major advantage of KEH-based gait recognition is the potential for significant [power](#) savings as it doesn't need to use the accelerometers at all.

As with any authentication technique there are security risks. For example, a signature can be forged, a pin number can be hacked and a password can be autosaved.

So how secure is KEH-Gait authentication?

Security test

To evaluate this we built two different KEH prototypes and experimentally validated the performance over 20 subjects with 200 gait cycles from each subject. Each subject participated in two independent data collection sessions.

Our data was collected in several environments (indoor and outdoor) including plain, grass and asphalt terrains, representing the natural gait changes over time and terrains.

[Our results](#) show that KEH-Gait can achieve an authentication accuracy of 95% and reduce energy consumption by 78.15%, compared to conventional accelerometer-based authentication techniques.

We also tested the robustness of the KEH-Gait system against an attacker trying to imitate someone's motions. Out of 100 imposter trials, we found that 13 were wrongfully accepted.

Some false positives can occur when the gait patterns of the imposter and the user are close. But the behavioural characteristic of human gait provides our scheme security against such attacks. Since KEH-Gait keeps authenticating the user continuously, it becomes more difficult to reproduce the [gait](#). Imitating how a person walk over time is extremely difficult if not impossible.

So by capturing movements that are unique to a user, KEH-Gait presents a secure, continuous and implicit authentication tool – a promising development given the booming wearable [device](#) market.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation

Citation: The way we walk can be used to power and secure our devices (2017, May 24) retrieved 10 April 2024 from <https://techxplore.com/news/2017-05-power-devices.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--