

Bitcoin wallet devices vulnerable to security hacks, study shows

January 23 2018



Credit: CC0 Public Domain

Devices used to manage accounts on the innovative payment system

Bitcoin could be improved to provide better protection against hackers, research suggests.

Computer scientists have identified security weak spots in gadgets that manage personal accounts using Bitcoin - a form of [digital currency](#) that provides an alternative to conventional money.

They also identified how these wallets - which are popular among the Bitcoin community - might be rectified. Their findings could help technology firms improve how the devices - known as Bitcoin [hardware](#) wallets - interact with our PCs.

A team at the University of Edinburgh carried out an in-depth security analysis of the communications system used in popular models of Bitcoin wallet.

They created a simple piece of harmful software, or malware, which was able to intercept messages sent between hardware wallets and computers - where users manage their Bitcoin accounts.

The tests revealed that users' privacy is not protected. They also showed how easy it is to access Bitcoin funds managed by such devices and divert them into a different [account](#).

Based on their findings, researchers proposed a fix for improving the [security](#) of such systems. This would encrypt particular messages sent between Bitcoin wallets and computers, making them much more secure.

Their fix could be incorporated into all models of Bitcoin hardware wallet to offer better protection against hacks, the team says. Their study is published in the journal *Information Security*.

Dr Andriana Gkaniatsou, of the University of Edinburgh's School of

Informatics, who led the study, said: "A [wallet](#) should protect not only our money, but also our privacy. It was surprising to discover how easy it is to access a user's funds, even when sophisticated hardware is incorporated.

"Unfortunately, there is no silver bullet when it comes to protecting financial digital assets - we need to ensure that all components of the system are equally protected and interact in a secure way."

Provided by University of Edinburgh

Citation: Bitcoin wallet devices vulnerable to security hacks, study shows (2018, January 23)
retrieved 9 April 2024 from

<https://phys.org/news/2018-01-bitcoin-wallet-devices-vulnerable-hacks.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>
--