# Computing expert finds way of securing Internet of Things

June 21 2017

Credit: University of Portsmouth

A computing expert has found a way of securing the Internet of Things,

a term that encompasses everything connected to the internet from smartphones to smart fridges.

Paul Fremantle, at the University of Portsmouth, analysed 55 systems for managing the Internet of Things (IoT), and found a large majority had no support for security or privacy, and few systems implemented robust controls.

This means the IoT is increasingly vulnerable to cyber-attacks, demonstrated last year when more than 100,000 IoT devices were taken over and used to attack the US internet, bringing down many of the systems across the East Coast.

Paul from the University's School of Computing has published a framework to show how blockchain technology, which is the basis of the Bitcoin currency, can be used to enhance the security, privacy and manageability of IoT devices and networks.

Paul said: "The IoT is all about connecting devices to a network and enabling them to collect and share data. It can include anything from household objects like thermostats, light switches, doorbells and fridges to toys, cars and medical devices.

"It's a real concern that we're buying these devices without thinking of the consequences. For example when you buy a fitness tracker it's hard-coded to the company that sold it. If their network isn't secure then your data isn't secure.

"Some of these smart devices can access incredibly rich data. Google Nest knows what room a person is in and whether they're asleep or awake. Monitors inside some of the latest cars can tell if a driver is male or female, or even whether the driver is pregnant.

"There aren't really strong incentives for manufacturers to update their systems to keep you safe, so you can easily be attacked personally – the brakes of your car could be hit while you're driving it – or your things could be taken over to attack something else.

"The first time the digital world affected the physical world was when a worm that became known as Stuxnet attacked a nuclear plant in Iran. This virus physically destroyed nuclear centrifuges which were separating different types of uranium.

"This was back in 2010, and now that virus is available to malware authors. It's quite frightening that there is a steady growth of the number of devices connected to the internet, but the lack of security remains a big concern. The only true privacy control a user has is often just to completely disable a device."

Paul's research proposes a model using blockchains, which were originally devised for the digital currency Bitcoin.

Blockchain is a method of recording data – a digital ledger of transactions, agreements, contracts – distributed across several, hundreds or even thousands of computers around the world.

He said: "Blockchains create a shared governance. They create an environment for IoT networks where there can be trust, anonymity and effective contracts between parties without any single vendor being in charge, and without requiring any party to be trusted above another."

Paul has proposed a number of ways in which blockchains can improve the security and privacy of the IoT. However, a challenge remains: the processing, memory and code requirements of blockchains makes them incompatible with cheap, constrained IoT devices.

One of Paul's proposals is a new approach that enables IoT devices to participate in a trusted blockchain. The proposal is to create a new system, called a Pythia that acts as a trusted intermediary between blockchains and the internet-connected devices.

Pythia is named after the priestess at the temple of Apollo in ancient Greece, who acted as a go-between between the gods and humans. With this system in place, IoT developers will be able to trust blockchains more easily, leading to many new approaches for a secure IoT.

He said: "My vision of a blockchain-based IoT is in the preliminary stages, but we plan to start prototyping it shortly. Unless we solve the security problems soon, there will only be more serious attacks coming."

Paul's paper was published at an international conference on Internet of Things, Big Data and Security in Porto, Portugal.

Provided by University of Portsmouth