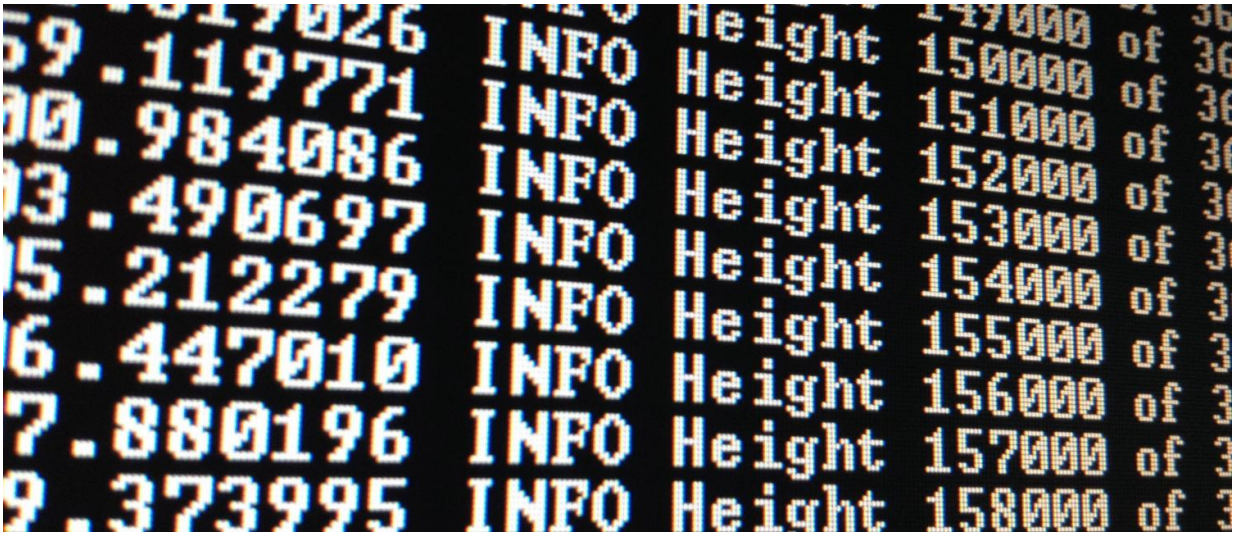
Blockchain making houses safer

August 16 2017, by Benedict O'donnell, From Horizon Magazine



Blockchain technology is helping keep appliances in smart homes safe from hackers. Credit: 'Blockchain' by deavmi is licenced under CC SA-4.0

Blockchain technology developed to guarantee the value of cryptocurrencies such as Bitcoin and Ethereum is now being adopted by engineers as a way to fight off the risk of a hacker breaking into the connected appliances of today's smart homes.

In recent years, domestic appliances smart enough to automate tasks ranging from ordering Christmas gifts to turning on thermostats have spread to millions of homes across Europe.

This increasing interconnection, often referred to as the Internet of Things (IoT), is attracting an eclectic range of enthusiasts. Yet according to Javier Augusto at Televes, an IT company in Santiago de Compostela, Spain, start-ups and tech firms are not the only ones exploring its opportunities – hackers are keen on the concept too.

'Each connected device opens a new crack in the security of a computer network,' said Augusto. 'It is unclear how safe the cybersecurity tools we have today can keep IoT devices. They were developed for internet protocols, not Bluetooth or 4G.'

Augusto raises concerns that intruders who break into connected products like activity trackers, smart fridges or fire alarms could spread across home networks to access bank credentials or eavesdrop on conversations.

Televes is coordinating the EU-funded GHOST project to lock down our home appliances through an electronic gateway that shuts out attacks.

'The gateway stands as a buffer between the smart appliances inside the house and the outside world,' he explained.

To make sure that the gateways themselves remain uncorrupted, the consortium is drawing on advances in blockchain technology.

Puzzle

'Blockchain is a piece of software that essentially crowd-sources oversight,' said Augusto. 'It works by giving lots of computers one piece of a puzzle that can only be solved as a joint effort.'

Whereas cryptocurrencies use blockchain to check that no two people spend the same coin, the GHOST project is adapting the software and

exploiting it to make sure that no outsiders tamper with the list of cyber threats hosted on its gateways.

GHOST partners have designed their gateways to record encrypted information on all other gateways in their network. To trick the blockchain, a hacker would have to commandeer half the machines in the network.

'In principle, blockchain technology guarantees that our security gateways remain clean and up to date,' said Augusto. 'This would be an unprecedented step forward in cybersecurity.'

He expects that the GHOST consortium will field-test the first features of their device in a 2019 prototype, and roll out the full technology by 2022.

Yet IoT doesn't only increase the risk of a cyber attack, according to Sergios Sousos at Intracom Telecom, a technology company in Peania, Greece, it also raises its stakes. Breaches into home computers may prove costly in money terms, he said, but remote tampering with a dialysis machine or a gas oven is a matter of life and death.

The first step towards bulletproofing the IoT is to open it up, according to Soursos. Although more appliances are becoming smart, he said that few are yet talkative – at least not with products developed by competitors.

Far from making them safer, this silo approach places each system at the mercy of its weakest link. One breach is liable to bring down an entire network of connected devices. It also wastes an opportunity for manufacturers to swap mutually beneficial data and develop more high-tech services.

'The probes in many alarm systems today know when their owner opens a window but have no way of switching off the smart air conditioning unit,' explained Soursos. 'Even if app developers wanted to make these machines work together, today they have no simple way of doing so. IoT devices do not even speak the same language.'

The symbIoTe consortium, funded by the EU and coordinated by Intracom, is developing software that helps IoT platforms work with one another. Homeowners can upload it to endow devices with the ability to broadcast what data they record and inspect the credentials of anyone trying to access them.

While not dealing with blockchain specifically, Soursos expects the symbIoTe add-on will be another tool to strengthen IoT security. One advantage of its interface is that it allows homeowners to define the sensitivity of functions performed by each machine, and how much authority is needed to activate them.

Provided by Horizon: The EU Research & Innovation Magazine

Citation: Blockchain making houses safer (2017, August 16) retrieved 2 May 2024 from https://techxplore.com/news/2017-08-blockchain-houses-safer.html