Cyberattack ‘Stops Hackers in Their Tracks’: World's First 'Uncrackable' Code Developed by Scientists

21/12/2019

While current cryptographic techniques are believed to be still at least one step ahead of those seeking to decode them, scientists have been sounding the alarm, as all this could dramatically change in the not too distant future with the arrival of quantum computers.

A team of scientists claim to have sensationally developed the world’s first “uncrackable” security system code, even capable of keeping the threat of quantum computers at bay.

In their research, “Perfect secrecy cryptography via mixing of chaotic waves in irreversible time-varying silicon chips”, published in the scientific journal Nature Communications on 20 December, the University of St Andrews scientists, together with international partners are believed to have achieved “perfect secrecy” with their new technology.

This has been achieved through developing a prototype silicon chip that uses the laws of nature, including chaos theory and the second law of thermodynamics. The cryptographic keys generated by the chip, are never stored and are not communicated with the message.

The digital information is first stored as light, subsequently passes through the silicon chip’s structures that bend and refract the light, scrambling the information.

First author, Professor Andrea di Falco of the School of Physics and Astronomy at the University of St Andrews, said:

> “It’s the equivalent of standing talking to someone using two paper-cups attached by string. If you scrunched up the cups when speaking it would mask the sound, but each time it would be scrunched differently so it could never be hacked.”

Thus, traditional methods of encryption hacking are rendered irrelevant, claim the scientists, as there is no software or code to manipulate.

What’s more, it is also touted as being able to overcome the threat of quantum computers and can do so using existing communication networks.

Although true quantum computers are still a long way off, security experts have been voicing concerns that cyber-terrorists might be already storing information for hacking once quantum computing becomes a reality.

> “With the advent of more powerful and quantum computers, all current encryptions will be broken in a very short time, exposing the privacy of our present and, more importantly, past communications,” said leader of the study, Dr Andrea Fratalocchi, Associate Professor of Electrical Engineering at King Abdullah University of Science and Technology, in Saudi Arabia.

The breakthrough technology, claim the scientists, would stop hackers in their tracks.

“This system is the practical solution the cybersecurity sector has been waiting for since the perfect secrecy theoretical proof in 1917 by Gilbert Vernam,” Dr. Al Cruz, founder of the Centre for Unconventional Processes of Sciences (CUP Sciences) in California, and co-author of the study said.

Summarizing the research as potentially capable of revolutionizing communications privacy, Dr. Cruz said:

> “We’re obviously very excited to finally be able to talk about the work,” Dr. Cruz says, “and now that we are out of the lab, the next phase is to engage with partners to help us explore the commercial possibilities.”