Encrypted Sensors

Media Contact:
Windy Campbell
(804) 314-0205

Virtual Private Networks (VPNs) are Hackable, according to Mueller Report. Introducing the World's First Actual Private Network (APN).

Richmond, VA (April 26, 2019) -- A hardware-based encryption system is considered by cybersecurity experts as a logical solution to virtual private networks (VPNs), the software-based networks that were broken into by the Russians in 2016.

Encrypted Sensors is the first cybersecurity company to program a quantum computer-proof encryption onto a Field Programmable Gate Array (FPGA) hardware chip. The company has applied to trademark it as an *actual private network* (APN), a hardware-based encryption system that functions without software controls or operating systems on which VPNs are based.

The company's non-algebraic encryption algorithm is considered by cybersecurity experts to be the next generation encryption solution.

“Since our encryption is not based on math, it challenges the way computers operate,” explains Brian Penny, inventor of the patented algorithm and co-owner of Encrypted Sensors. “Any computer trying to break it would have to decide what is - and isn't - reality.”

As described in The Mueller Report, the Democratic Congressional Campaign Committee (DCCC) and Democratic National Committee (DNC) relied on VPNs. The report cites, on p. 38:

> *Approximately six days after first hacking into the DCCC network, on April 18, 2016, GRU officers gained access to the DNC network via a virtual private network (VPN) connection between the DCCC and DNC networks. Between April 18, 2016 and June 8, 2016, Unit 26165 compromised more than 30 computers on the DNC network, including the DNC mail server and shared file server.*

“This showcases one of the main problems with virtual private networks,” said B.K. Fulton, an advisory board member of Encrypted Sensors and a former regional vice president of Verizon Communications, Inc. “Because VPNs are software-based, they can be tricked by software to allow access. In most cases, a simple password will allow access. If the DCCC wants to stop these kinds of security problems in the future, they need to start using actual private networks. APNs highly disruptive, patented encryption technology will further eliminate the anxiety over possible computer hacking.”

-- more --

Hardware-based APNs function independent of any software controls or operating systems. An attacker would have to physically gain control of the specific APN hardware that is set up for the network.

Benefits of the encryption being on the FPGA chip include having control of the entire encryption environment. The encryption can run a lot faster, near real time, compared with other encryption systems.

For more information on Encrypted Sensors, including its founding members and advisory board, please visit http://encryptedsensors.com/.

###

About Encrypted Sensors

Founded in 2018 with headquarters in Richmond, Va., Encrypted Sensors is powered by a patented, non-algebraic encryption algorithm that works at the bit level. Encrypted Sensors' innovative approach provides a proactive cybersecurity solution for America.