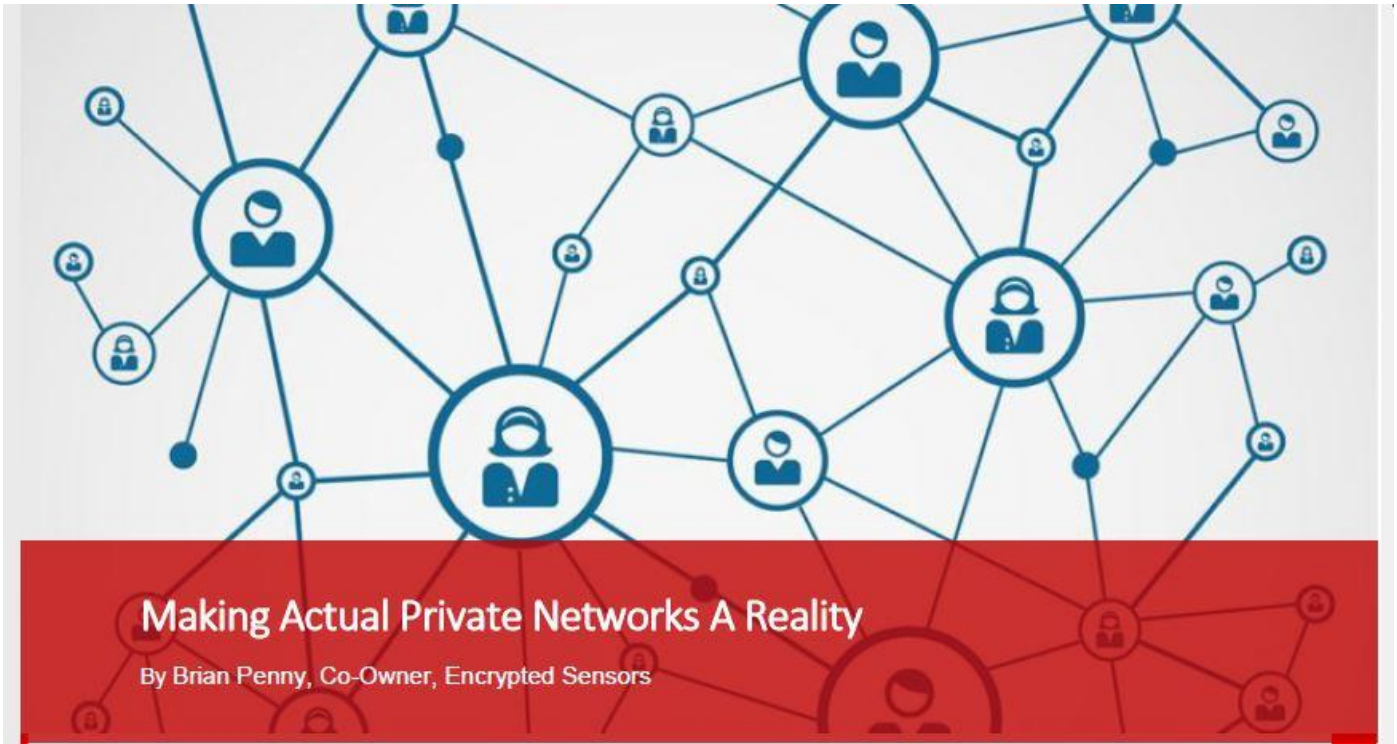

CDM
eMAGAZINE
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
IN THIS EDITION
WMD vs. Cyber Attacks: Similarities Suggesting
Why Federal Agencies Need AIOps
Safeguarding Your Organization from Attacks via Your Third-Party Vendors
Cyber Security Facts and States For 2019
Threat and Incident Response
Ransomware: Are We Really Prepared For Cyber-Attacks?
You're Guide to Encrypting Files in Linux
JUNE 2019
MORE INSIDE!



Making Actual Private Networks A Reality

By Brian Penny, Co-Owner, Encrypted Sensors

Virtual private networks (VPNs) have long been considered the bread-and-butter of enterprise security. VPNs were designed to funnel all user traffic through an encrypted, secure, private network, making it more difficult for a third party to monitor browsing than if the data were exposed on a public network. However, VPNs are still vulnerable to intrusion, thanks to hackable software in which VPNs are placed.

Software-based VPNs a national security risk

Several notable security risks and flaws of software-based VPNs have come into light in recent months. In April 2019, the Mueller report revealed that the Russian Intelligence Agency (GRU) in 2016 gained access into the data, files and emails of the Democratic Congressional Campaign Committee (DCCC) and Democratic National Committee (DNC), through the VPN which supported the organizations' network computers. The Mueller report, on page 38, cites:

> *"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."*

Around the same time when the Mueller report findings were revealed, the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security in April 2019 issued an

alert after CERT/CC revealed that several enterprise VPN apps built by four vendors — Cisco, Palo Alto Networks, Pulse Secure and F5 Networks – contain a security bug that can allow an attacker to remotely break into a company's internal network. Scores of other VPNs may be affected, as well.

Considering these vulnerabilities, why risk the potential for intrusion and future hacking? A solution is finally here.

The "Next Generation" of encryption systems

Cybersecurity company Encrypted Sensors is the first to program a quantum computer-proof encryption onto a Field Programmable Gate Array (FPGA) hardware chip. Unlike the software-based VPNs, the encryption is run on hardware and functions without any software controls or operating systems upon which VPNs are based.

This non-algebraic encryption algorithm is considered by cybersecurity experts to be the next generation encryption solution. Because the encryption is not based on math, it challenges the way computers operate. Any computer trying to break it would have to decide what is - and isn't - reality.

Encrypted Sensors has applied to trademark its encryption system as an *actual private network* (APN).

"The security risks revealed in the Mueller report and elsewhere showcase one of the main problems with virtual private networks," said B.K. Fulton, an advisory board member of Encrypted Sensors and a former 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 government agencies and enterprises want 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."

As an encryption system that is hardware-based, APNs function independently without 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 APN

Being programmed into an FPGA chip awards the APN encryption numerous benefits. The APN controls the entire encryption environment. The APN encryption can run a lot faster, near real-time, compared with other encryption systems. This allows for encrypted secure connections in new places like drones,

wearables and any sensor-type system. Running on a stand-alone FPGA chip, the encryption is already configured thus greatly reducing potential user error.

The Solution Awaits

APN's plug-and-play functionality with TCP/IP devices allows an end user to secure legacy systems alongside newer technology. For example, voting machines all over the nation are at vastly different stages of technological development. A machine from the 1990s that lacks interface with modern networks is a giant welcome sign to hackers wanting access. Thus, having an APN always encrypting every single bit going in and out of the machine creates a physical barrier from cyber intrusion.

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

About the Author

Brian Penny is co-owner of Encrypted Sensors and the inventor of its patented algorithm. As a musician and sound engineer, Brian shares a passion for sound design, which led him to tampering with clocks to create unusual sounds. He combined binary word lengths and clocks to create Encrypted Sensors. Brian can be reached online at bripenny@gmail.com and at the Encrypted Sensors website http://encryptedsensors.com/.