CoreVUE

Breakthrough in Cybersecurity – Dynamic Key Management

High Level Description

www.TunnelVUE.com

Breakthrough in Cyber Security - Dynamic Key Management

Enabling Encryption Everywhere

By Richard Plaskett, MSA

The DoD is in the throes of a rapidly expanding cybersecurity problem. According to *Cyber Security for Defense*, "The DoD accounts for the largest share of the total U.S. cybersecurity budget, with a reported $8.5 billion in cyber funding in FY 2019, which is a $340 million (4.2 percent) increase from 2018. This funding will go towards activities such as the Pentagon's efforts to defeat enemy cyber-attacks against U.S. forces and the military's abilities to conduct cyber warfare against existing and potential adversaries."[1] Clearly this is a significant, growing problem for which many different solutions exist which are costly and labor-intensive provide varying degrees of security. Few provide real assurance.

It is widely acknowledged that encryption is the single best method to protect data.[2] Using today's encryption methods there is a near-zero chance that encrypted data can be exploited (until quantum computers become widely available). But there are substantial barriers to enabling encryption across whole systems largely due to:

- Current doctrine treats network infrastructure as inviolable; however, costs to fully protect are too high and the resultant security is still too imperfect
- All IT systems in the enterprise security apparatus require *human* interface, introducing high probability of errors and/or willful circumvention of "the rules" for sake of expediency
- DoD systems are far too complex, requiring multiple solutions which each require unique configurations, specialized training, and an unending logistics/cost (after cost to implement)
- The move to IT and Cyber Security as a service provided by commercial vendors will likely *not* provide even the degree of caretaking that already exists

Thus, we know that encryption is in fact, *not* enabled where it is truly prudent to do so, and many critical government systems remain subject to interception, hacking, and malicious cybercrime.

[1] *cybersecurityfordefense.iqpc.com* *enquiryiqpc@iqpc.com* *1-800-882-8684*

[2] *https://www.eetimes.com/document.asp?doc_id=1279619#*

Richard Plaskett, Director of Communications, Tunnel Vue, Inc. **richardplaskett@tunnelvue.com** **text or voice: 334-657-9986**

But, from an almost accidental collision of need, opportunity, and creative thinking by the right people, we have the only solution that actually *eliminates* the usual infrastructure-dependent models.

Tunnel VUE, Inc. was founded to simplify the use of encryption for data-in-motion with a revolutionary post-quantum encryption key management system that eliminates need for PKI or other asymmetric key management systems used in today's solutions, while allowing universal encryption of all data in transit with no hands-on management including configuration of routers, switches, etc. Simply put, it allows *extremely robust encryption, everywhere, inexpensively.* In this one product we have accomplished the following:

- Fully-automated, zero-provisioned dynamic encryption key management; 100% software-based
- "Multifactor postquantum methodology"[3] wraps every packet in an encrypted session (including the very first packet) with a separately-established, unique key for each session *and* a unique key for every packet within each session.
- Zero human intervention required for key management, distribution, storage, or usage
- Replaces PKI, ISAKMP, IKE and other asymmetric key management tools - no key management
- Essentially agnostic to operating systems, hardware and resident software. It renders infrastructure as a commodity, to be managed only as a system of networks
- Network attack vector limited to a single zone, versus every connection point on the network
- Prevention of lateral activity in any network, thus, non-propagation of malware/zero-day exploits
- Total attribution of every transmission to its exact source and time

Note that CoreVUE does not implement a new encryption algorithm, nor does it establish a new random key generator. CoreVUE manages industry standard and universally accepted solutions such as AES, IPSec, and FIPS140-2 certified key generators for these functions.

We would be happy for you to send cybersecurity experts to visit our lab in Montgomery, Alabama for a demonstration—or we can come to you. We understand that what we claim about our product seems incredible. We welcome any expert you would send to visit our lab to see the proof, which we are keeping closely guarded.

[3] *Panoyatis Yannakogeorgos, PhD. Founding Dean, Air University Cyber College*

Richard Plaskett, Director of Communications, Tunnel Vue, Inc. richardplaskett@tunnelvue.com **text or voice: 334-657-9986**