CoreVUE

Confidentiality, Integrity, & Availability Through Universal Symmetric Encryption

High Level Description

www.TunnelVUE.com

CoreVUE's technology simplifies the protection of data in transit using a revolutionary post-quantum encryption key management system that eliminates the need for PKI or other asymmetric key management systems used in today's solutions, while allowing universal symmetrical encryption of all data in transit with no hands-on management including configuration of routers, switches, etc. Turning on universal symmetric encryption using the CoreVUE model can positively impact the three primary goals of cyber security of confidentiality, integrity, and availability.

Hallmarks of Universal Symmetric Encryption
• Be installed on ALL systems in a subject network. • Employ symmetric encryption technologies exclusively. • Act against all packets transmitted by subject systems. • Ensure positive identity of all systems. • Not introduce any factor that reduces entropy in the network. • Provide forensic level attribution of all packets. • Provide well defined and limited number of inspect points in the network.

CoreVUE is a dual-layer, dynamic, symmetric, post-quantum key and encryption management methodology. CoreVUE does not use any asymmetric encryption for key exchange such as public key infrastructure (PKI). Instead, CoreVUE uses a dual encryption methodology that implements a different key for each session on a device as well as a different key for each packet within each session. Every system uses completely different keys. Effectively employed, the CoreVUE encryption cycle begins below the protocol stack, as an endpoint device communicates back to a "trusted zone" such as a datacenter or security monitoring point. This effectively prevents access to the kernel. Within the trusted zone encrypted traffic either is decrypted and sent back within the internal network to access resources as allowed by security policies or, out to the internet in its original form. CoreVUE's small footprint (less than 50 KB) and its ease of integration to any software platform—including operating systems, software applications, or network connected electronic system endpoints—allows adoption by any electronic device connected to a network.

CoreVUE has an *absolute* effect on **confidentiality** as 100% of all traffic is "intercepted" and encrypted with independent keys by the dynamic key manager. This means that even if data is able to escape the confines of the internal network, or malicious actors have physically infiltrated the network the data will remain confidential. Confidentiality is accomplished by a dual-layer key system that requires an attacker to break both the session key and the packet key simultaneously. This can only be accomplished by a brute force attack. Assuming the use of a 128-bit session key and 128-bit packet key, CoreVUE would achieve an equivalent key space of 256 bit which is comparable to current standards. Each packet is first fully encrypted with the dynamic packet key that changes with each packet, and then it's encrypted again via the session key. This requires an attacker to run the entire key space for every packet key for each iterative attempt to break the session key, because without *both*, an attacker is unable to determine if the session key is correct. Without the packet key, the data decrypted by the potential session key remains encrypted and useless. With each underlying packet key being different than every other packet key there is no way to find commonalities between packets to aid in decryption. This allows data protected with CoreVUE's methodology to remain confidential even into the quantum age, since CoreVUE's dynamic dual-layer methodology is not subject to existing quantum algorithms.

CoreVUE's methodology delivers a *dramatic* effect on **integrity** because 100-percent of all traffic is encrypted using the dynamic key manager. Implemented correctly, the dynamic key manager would be

fully aware of all provisioned clients in the subject network, and the keys issued to the clients would be unique to each client. This means that only the device that sent the data and the trusted zone can decrypt or encrypt the message *between each other*. Due to the nature of the dynamic key manager the successful completion of a encrypt/decrypt cycle establishes undeniable attribution of every packet at a forensic level as only the two machines currently engaged in communication know the current session and packet key. When combined with an identity management system such as active directory, the result is absolute forensic level nonrepudiation of actions conducted from all machines on the network. Any Corruption or alteration of the packet either accidental or malicious results in rejection of the data and a request for retransmission from the application layer. With all these factors in place it is possible to determine that every usable encrypted packet that arrives at either an endpoint or trusted zone has perfect integrity.

CoreVUE also has a *positive* effect on **availability** throughout the network. The effect is gained through several factors:

The first is by simplification of network design and configuration. With every approved packet encrypted any Access Control List (ACL) established for internal activity can be reduced to two lines; the first being “allow encrypted traffic” and the second being “deny all”. This causes a significant reduction on the load of processing within the infrastructure. Next is a reduction of complexity of design because all traffic is effectively transmitted in an encrypted VLAN so routers and switch VLANs can be eliminated, allowing approved traffic flows direct access to the trusted zone. This also reduces the need for long complex downtimes for equipment replacement or modification. Configuration could be as simple as assigning a management IP, change the default password and plug in the existing cables. Universal encryption also eliminates the need to update infrastructure operating systems (i.e. switches, routers) because of discovered vulnerabilities since the unbreakable packet reduces the defense of infrastructure to simple physical network security. This would eventually lead to the network infrastructure being treated like the electrical infrastructure of building, requiring attention only during installation and system failure.

The second factor is that since all traffic to and from a device is encrypted, any invalid attempts to communicate with a device will be discarded after the decrypt process fails. This fact means that an attempt to gain control over a system for the purpose of subverting the functionality of the system will always fail. Having a universally encrypted network means that no system attached to the network could be used to start an active denial attack against the internal infrastructure of the network, leaving the only avenue of attack through subversive introduction of non-encrypted systems. This threat is easily eliminated through the use of the deny-all ACL and continuous monitoring for unencrypted sources of traffic.

Finally, in the universally encrypted network the possibility of lateral attacks is significantly reduced. Since every packet issued by a device would be routed to the trusted zone for decryption and management, lateral movement is controlled through the natural application of common-sense rules. In this kind of network any exploratory packet issued by a zero-day threat would be moved to the trusted zone first where the security systems should easily identify and eliminate the threat. Finally, your security personnel can shift their focus to the single point in the network where EVERY packet is readily accessible.