Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability

Nicholas Edwards
Tunnel VUE

Sara Bliss Kiser
Alabama State University

Janel Bell Haynes
Trenholm State Community College

Protecting the flow of sensitive information processed on computers is a challenge facing cybersecurity professionals. This proof of concept uses universal encryption of all data in transit with no hands-on management. This revolutionary process secures data in a virtually unbreakable system protecting the flow of data unlike any system available.

Keywords: cybersecurity, integrity, PKI, encryption

INTRODUCTION

Protecting the flow of sensitive information processed on computers is the single most difficult challenge facing cybersecurity professionals in today's market. With the advent of this challenge evolves an ever expanding and lucrative market.

There are more than 1000 companies in this $70 billion market (SalesInside, 2018). Due to the rise in cybercrimes and malware attacks on governments, banking, financial, security and insurance (BFSI) and healthcare organizations the marks projected to reach $198 billion by 2022 (Grand View Research, 2018). Juniper Research reports that the global cost of data breaches will rise to $2.1 trillion by 2019 (Irwin, 2017). Last, Drolet (2017) noted, "the Internet of Things remains a major weak point for defenses. … This in turn is giving rise to botnets, which can be used for volumetric attacks, to exfiltrate stolen data, to identify further vulnerabilities, or for brute force attacks" (para 8).

This research and resulting proof of concept prototype has created technology that 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. The research uses universal encryption of all data in transit with no hands-on management including configuration of routers, switches, etc. (Tunnel Vue, 2019). This revolutionary process secures data in a virtually unbreakable system that protects the flow of data unlike any system on the market today.

Businesses and Government

In 2018, American technology conglomerate Cisco (2018). reported that 53 percent of midmarket companies have experienced technology breaches and these firms only investigate 55.6 percent of the breaches which cost 20 percent of companies from $1 million to just under $2.5 million. Over fifty percent cost more than $500,000 "including, but not limited to lost revenue, customers, opportunities, and out-of-pocket costs" (p. 3). Cisco (2018) also reported that 40 percent of companies with 250-499 employees reported eight or more hours of downtime after a breach. To fight cybersecurity challenges small business reported that they would be most likely to "upgrade their endpoint security … [and] deploy intrusion prevention" (p. 7). Paine (2018) stated, "As cybersecurity continues to grow mainstream and to command the attention of consumers and companies alike, we'll continue to see late adopters seeking out cybersecurity specialists to update their antiquated systems and to bring them into the 21st century. This long tail represents a huge amount of buying power" (para. 10).

Research in this area stretches across the globe. The most recent Ponemon Institute study, sponsored by Raytheon, of security professionals in the U.S., Europe, Middle East, and Africa, shared their thoughts on the major issues to focus on in the next three (3) years. Some of the key findings were:

- 82% of respondents predict their workplace will suffer a catastrophic data breach in the next three years as a result of unsecured IoT devices. 66% say such an attack would seriously diminish shareholder value.
- 46% believe their cybersecurity strategy will improve, down from 59% in 2015.
- 60% expect their companies will have to spend more to achieve regulatory compliance and respond to lawsuits and litigation.
- 43% of respondents rate the risk of breaches involving high-value information as very high and 71% of respondents say the risk will be very high over the next three years (Ponemon Institute, 2018).

> An Accenture (2017a) study found 59 percent of financial service institutions said it took months to find breaches and they are not being found by their security teams (64 percent), but by their employees, law enforcement, or ethical hackers. Financial services institutions note an average of 85 attacks a month with a third of them being successful. Alternatively, the energy sector feel they are secure; however, Accenture results disagree with that assessment. Accenture (2017c) reports "… oil and gas companies second to last in a cross-industry evaluation of high-performance cybersecurity capabilities …" (p. 2). Oil and gas executives report 86 attempted breaches a month (Accenture, 2017c).

There are 90,056 local governments per the 2012 Census of Governments (Governing, n.d.). Governments must protect themselves from further threats such as Petya which "infect[ed] computers and networks in more than 65 countries including the United States" (Hunt & Ahluwalia, 2017). According to a recent Accenture (2017b) survey, "Governmental organizations face dozens of focused, targeted attacks each year, one in three of which result in a successful security breach" (para. 3). The Accenture (2017b) survey of 150 federal, state and local government executives found: "nearly 70 percent of federal respondents (and around 40 percent state and local respondents) consider cybersecurity a top priority that they have completely embedded in their culture, most also admit that attacks are often unpredictable" (p. 2). Accenture (2017a, b) noted seven areas of concerns for agencies. The most important is Investment Efficiency. And the greatest place to focus according to "two-thirds of state and local respondents" is "end-point/network security and threat intelligence as most needed abilities (similar to commercial respondents)" (Accenture, 2017b, p. 3). A 2018 report by Security Scorecard (2018) (n = 655 local, state, and federal agencies) went as far as to look at the government cybersecurity posture in swing states like Florida, Ohio, Nevada, and New Hampshire. When it came to Endpoint Security, Florida, Ohio, and Nevada received an F, while New Hampshire received an A.

E-Commerce

E-commerce is another vital area facing data breach challenges. The numbers for e-commerce reported by vpnMentor (2018) show the staggering amount of money being spent online. In the United States, in 2017, Americans spent $660.4 billion. The Asia-Pacific market spent just over $1 trillion. Western Europe spent $432.6 billion while central and Eastern Europe spent $73.1 billion. Lastly, Latin Americans spent $71.6 billion and those in the Middle East and Africa spent $51.4 billion. The global numbers for e-commerce are expected to have grown 181.3 percent by 2021. In 2015, $1.592 trillion was being spent. The expectation for 2021 is $4.479 trillion (vpnMentor, 2018). Much of the financial information of these companies and the patrons in this sector is vulnerable to breach and out right attack.

THE NEW ANSWER TO CYBERSECURITY

The research presented here – 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). Effectively employed, the 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. 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. The product developed has a small footprint (less than 50 KB) and its ease of integration to any software platform allows adoption by any electronic device connected to a network.

CoreVUE has an *absolute* effect on **confidentiality** as 100 percent of all traffic is "intercepted" and encrypted with independent keys by the dynamic key manager. 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 a hacker to break both the session key and the packet key simultaneously. This can only be accomplished by a brute force attack. An attacker would have 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. Data protected with this new technology remains confidential even into the quantum age as it 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 will be aware of all provisioned clients in the subject network, and the keys issued to the clients will 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*. 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. These factors ensure 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 due to several factors. The first is the simplification of the 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" reducing the processing load within the infrastructure. Next is a reduction of the throughput complexity because all traffic is effectively transmitted in an encrypted VLAN allowing approved traffic flows direct access to the trusted zone. This reduces the need for long complex downtimes for equipment replacement or modification. Universal encryption also eliminates the need to update infrastructure operating systems (i.e. switches, routers) because the unbreakable packet reduces the defense of infrastructure to physical network security. This would eventually lead to the network infrastructure being treated similar to the electrical infrastructure of a building requiring attention only during installation and physical failure.

Second, since all traffic to and from a device that is encrypted, any unauthorized attempts to communicate with a device will not be encrypted and be discarded as garbage. This means any 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, security personnel can shift their focus to the single point in the network where EVERY packet is readily accessible (Tunnel Vue, 2019).

REFERENCES

Accenture. (2017a). *High performance security Report 2016: Building confidence: Solving banking's cybersecurity conundrum*. Retrieved from https://www.accenture.com/t20170216T011141__w__/us-en///www.accenture.com/t20180228T105508Z__w__/us-en/_acnmedia/PDF-44/Accenture-Building-Confidence-Solving-Banking-Cybersecurity-Conundrum.pdf#zoom=50

Accenture. (2017b). *High performance security Report 2016: Public Sector: Confidence + Capability: "Rebooting" public sector cybersecurity*. Retrieved from https://www.accenture.com/t20170215T210156Z__w__/us-en/_acnmedia/PDF-37/Accenture-Confidence-Capability-Rebooting-Public-Sector-Cybersecurity-RESEARCH.pdf#zoom=50

Accenture. (2017c). *Outside the (black)box: Protecting core operations – Energy Industry*. Retrieved from https://www.accenture.com/us-en/insight-building-confidence-cybersecurity-oil-gas

Cisco. (2018, July). *Small and mighty: How small and midmarket businesses can fortify their defenses against today's threats*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

Drolet, M. (2017, December 11). *8 cybersecurity trends to watch for in 2018*. Retrieved October 25, 2018, from https://www.csoonline.com/article/3241242/data-protection/8-cybersecurity-trends-to-watch-for-2018.html

Governing. (n.d.) *Number of governments by state*. Retrieved October 28, 2018, from http://www.governing.com/gov-data/number-of-governments-by-state.html

Grand View Research. (2018, February). *Cyber security market size, share & trends analysis report by component (solution, services), by security type, by solution, by services, by deployment, by application, and segment forecasts, 2018 – 2024 – Report summary*. Retrieved from https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Hunt, G., & Ahluwalia, L. (2017, August 3). *The cybersecurity strategies governments need*. Retrieved from http://www.governing.com/gov-institute/voices/col-cybersecurity-strategies-governments-need.html

Irwin, L. (2017, August 30). *Global cost of data breaches will rise to $2.1 trillion by 2019*. Retrieved from https://www.itgovernanceusa.com/blog/global-cost-of-data-breaches-will-rise-to-2-1-trillion-by-2019/

Paine, J. (2018, February 26). *5 cybersecurity trends to watch in 2018*. Inc. Retrieved from https://www.inc.com/james-paine/dont-miss-these-5-cyber-security-trends-in-2018.html

Ponemon Institute. (2018). *2018 Study on global megatrends in cybersecurity*. Retrieved from https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf

SalesInside. (2018). *Cyber security companies market share*. Retrieved October 28, 2018, from https://www.salesinsideinc.com/cyber-security-companies-market-share

Security Scorecard. (2018). *2018 Government cybersecurity report*. Retrieved from https://explore.securityscorecard.com/rs/797-BFK-857/images/2018%20Government%20Cybersecurity%20Report.pdf

Tunnel Vue. (2019*). CoreVUE: Confidentiality, integrity, & availability through universal symmetric encryption*. Retrieved May 30, 2019, from https://img1.wsimg.com/blobby/go/f66cc185-9213-4a09-9ae7-6915a8736d69/downloads/CIA%20-%20DC%20Second%20Round.pdf?ver=1558552531563

vpnMentor. (2018). *Internet trends 2018. Stats & facts in the U.S. and worldwide*. Retrieved October 26, 2018, from https://www.vpnmentor.com/blog/vital-internet-trends/