Encryption to see rise in adoption across all verticals

By Sunil Ravi

The importance of encryption

Encryption is a necessity of modern applications, given the migration of applications to cloud environments, and a growing trend of applications adopting the Software as a Service (SaaS) model. Applications must ensure that the data is encrypted while it is in transit and while the data is at rest using strong cryptographic ciphers and algorithms. Lack of strong encryption of data will render the application insecure and lead to confidential data of users/enterprises being breached by malicious attacks.

Data in transit needs to also incorporate the latest protocol versions (e.g., TLS v1.2 or later, SSHv2, IPsec, etc.) and avoid using old/deprecated protocol versions that are weak.

A majority of mobile and desktop applications also enable encryption by default. For example, all major browsers make an HTTPS connection by default when users visit any website, forcing websites and web applications to enable encryption. Additionally, all messaging applications such as Outlook, WhatsApp, Slack, Zoom, etc., have enabled end-to-end encryption, even with peer-to-peer messaging. Apple has also introduced the Advanced Data Protection feature which provides encryption of data at rest in the cloud.

Therefore, even end users expect encryption to be enabled for data in transit and data at rest, while using applications.

Applications need to enable encryption, by default, due to the changing landscape of how data is accessed – both personal and business. As more applications are deployed in the cloud with a SaaS delivery model, and those applications are being accessed using personal devices that may not have been properly secured by the enterprise, encryption becomes a significant first line of defense from a security posture.

Encryption with strong ciphers and algorithms, latest encryption protocols/versions, coupled with certified products (e.g., FIPS) and strong Public Key Infrastructure (PKI) is a foundational building block for modern applications.

The evolution of encryption technologies – where are we headed?

IPsec has been the protocol of choice for bulk encryption of data in transit, because IPsec uses UDP for transport. The IPsec protocol is used for establishing virtual private network (VPN) connections. Transport Layer Security (TLS) protocol is the protocol of choice for TCP-based internet protocols, such as HTTP, SMTP and LDAP. TLS has also been used for VPN connectivity as well, which is also known as SSL-VPN. TLS has also been adapted to use UDP as the transport protocol, which is known as DTLS. Popular SSL-VPN products use a combination of both TLS for TCP and DTLS for UDP to provide end-to-end encrypted communication.

Looking into the future, the trends indicate increased adoption of encryption in all applications. Major factors contributing to these trends include adoption of IaaS, PaaS and SaaS delivery models; remote/hybrid work environments; increased cybersecurity attack surface; and the increased cost of successful cybersecurity attacks. For example, DNS traffic is also being encrypted using DNS-over-TLS or DNS-over-HTTPS, as these protocols are supported by all major browsers. While IPsec, SSH and TLS are the dominant encryption protocols, certain innovations like SD-WAN provide secure overlay networks over multiple locations, with end-to-end encryption. Also, for data-at-rest encryption, there are several options being made available at the hardware, Operating System, and Application level. With the incorporation of stringent cybersecurity and privacy laws by various Government, Legal and Regulatory entities, the cost of successful data breach increases manifold – therefore there is an increasing trend across application deployment teams to enforce encryption of data at rest.

Finally, the ciphers and algorithms that are currently in use in modern cryptography are themselves at risk of being defeated with the advent of Quantum Computing. Current cryptographic operations rely on the assumption that certain mathematical operations, like integer factorization and discrete logarithms, take a very long time even for modern computers. However, Quantum Computing can solve such complex mathematical operations within a finite amount of time. Advances in Quantum Computing pose a significant threat to encryption technologies that are currently deployed. With increased awareness among enterprises regarding the threat posed by Quantum Computing innovations, there is a trend to replace existing encryption technologies with Quantum Computing Resistant (QCR) cryptography.

As Chief Security Architect at Versa Networks, Sunil performs multiple roles contributing to the overall security of its products and services. He has been a key contributor to the architecture of Versa software that provides deep integration of various network and security functions of the Versa Secure SDWAN and SASE solution. He has built up the core Security Operations that span Security Research, Secure SDLC, CI/CD, DevSecOps for rapid delivery of various products / services that are part of Versa's SASE solution.