TLS ATTACK SURFACE REVIEW

ENTERPRISE ENCRYPTION CHALLENGES

Encrypted communications are becoming ubiquitous within enterprise organisations as an enabler for modern standards and best-practice for security and privacy. Organisations have been deploying encrypted communications for the past 15 – 20 years, which continues to spread as organisations accelerate the digitisation of services and applications. Protection of an organisation's critical data and ensuring regulatory compliance and privacy of the data have never been more important.

When implemented correctly, encryption provides enhanced security and privacy for sensitive data and application traffic. Not identifying and validating your encrypted landscape is analogous to not understanding your server patch levels or exposed vulnerabilities. You cannot apply appropriate policy or action to what is unknown.

Many organisations do not have a defined standard for encrypted communications, and for those that do, the validation of such benchmarks is frequently not checked or maintained. For example, some organisations use static analysis of servers to check the certificate. However, this does not provide any clarity, reporting or assurance of the encrypted communications that are actively in use "in-flight" in an organisation's networks, its supply chain or its communications with employees and end-users.

Traditional network technologies fail to cater to this rise in encrypted traffic creating new challenges for security, privacy, and risk teams. Weak or vulnerable connections can lead to threat actors leveraging vulnerabilities to hide within encrypted communications and exploit the servers/applications. Attackers have also capitalised on this lack of visibility and have modified their methods for data exfiltration tools to operate within encrypted traffic flows.

In recent years, regulators have specified that data-in-transit be encrypted, meaning that global organisations adhere to TLS 1.2 or better. Ultimately creating challenges for global organisations as they now need the mechanisms to validate that the traffic for specific services, applications or regions are encrypted to the respective regulations. It is now essential that strong encryption is continuously monitored internally and across the organisation's supply chains.

As multiple parts of an IT organisation may be responsible for deploying certificates and encryption protocols, it has become challenging to identify misconfiguration and associated risks. Now more than ever, it's critical that security and compliance teams set strong encryption standards and continuously monitor communications to minimise risk to the organisation.

WHAT IS A TLS ATTACK SURFACE REVIEW (ASR)?

The Venari Security TLS Attack Surface Review (ASR) analyses and assesses the encrypted traffic communications across your entire infrastructure including datacentres, private cloud, or specific targeted areas to highlight the state of encryption used within your environments. The Venari Security Sensor is a virtual software appliance easily deployed in under ten minutes. Our VigilanceAI platform only gathers metadata associated with the network traffic, always maintaining the privacy of your data as no decryption takes place.

It delivers clarity to the privacy, risk, compliance, and security teams of your encrypted communications. For example:

- Are the appropriate cipher suites used to ensure strong encryption?
- Are the communications truly encrypted?
- Are the TLS versions being used outdated or vulnerable?
- Are there any connections to known bad sources within your encrypted traffic flows?
- Are there any expired certificates or certificates due to expire in the next 30 days?

The key stakeholders receive a report of the findings for them to understand whether they meet their internal standards. This allows you to benchmark against regulatory and privacy controls and ultimately allow your teams to prioritise and remediate risks based on the findings.

WHAT IS A TLS ATTACK SURFACE REVIEW (ASR)?

Any organisation's digital transformation investment is significant, and TLS is widely adopted. As attackers use encryption to hide, assuring encrypted communications becomes essential.

For the first time, this report highlights the status of an organisation's use of encryption across the entire environment including cloud and third-party environments.

Here are some examples of the risks found within organisations:

- Identify old and out-of-date SSL/TLS versions and the associated infrastructure.
- The use of deprecated or out-of-date protocols.
- Vulnerabilities within specific encryption protocols.
- The use of weak encryption
- Sessions that have negotiated null payload encryption.
- Weak or vulnerable public key distribution.
- Self-signed certificates used on production or other business-critical platforms.
- Certificate expiry and long-life certificates that do not conform with standards.

WHO BENEFITS FROM THIS TYPE OF ASSESSMENT?

Multiple stakeholders benefit from this service:

- CIO - The report allows the CIO to visualise the risk of poor encryption standards and strengthen encryption standards across the business.
- Privacy Teams - Maintain strong customer, employee, and transactional privacy for any inflight encrypted communications.
- Risk and Compliance - Ensure that all regulated services maintain encryption based on the defined standard and report back to executive teams for specific governance and risk controls.
- IT Security - Enables the CISO and the security team to gauge how secure the encrypted traffic is and where the priorities for resolution lie.

Encryption can create overhead and latency in applications, ensuring strong standards are maintained and that encryption protocols are appropriately and correctly configured across applications and services can enhance application performance.

WHY SHOULD YOU TAKE ON THIS SERVICE?

Organisations should conduct a TLS attack surface review as part of their routine security hygiene activities. Historically, it has been a challenge to understand and analyse the encrypted traffic across an organisation's infrastructure, causing it to be neglected in security and risk assessments.

This challenge is increasing in scope and difficulty as the use of encryption continues to grow. Venari Security now provides organisations with the ability to validate internal and regulatory encryption standards without decryption. Providing significant value over current security, and IT assessments translating into significantly reduced risk exposure and the attack surface for our clients.