REPORT ON LEGACY OPENSSL CIPHERS AND THEIR DEPRECATION

INTRODUCTION

In the realm of digital security, cryptographic ciphers are the bedrock of secure communication protocols like SSL/TLS. Over time, as computing power increases and cryptanalytic techniques advance, older ciphers that were once considered secure can become vulnerable. OpenSSL, a widely used cryptography toolkit, supports a vast array of cipher suites. Many of these are now considered "legacy" or "old-school" due to inherent weaknesses that make them unsuitable for modern security standards.

COMMON LEGACY CIPHERS AND THEIR WEAKNESSES

Several algorithms and cipher suites have been deprecated or are strongly discouraged for use today:

1. RC4 (RIVEST CIPHER 4)

- **Weaknesses:** RC4 is a stream cipher that suffers from significant biases in its output. These biases can be exploited by attackers to recover plaintext information, especially after observing a large amount of ciphertext. It is also susceptible to keystream reuse attacks, which can reveal the entire key.
- **Commonly Found In:** Cipher suites like `TLS_RSA_WITH_RC4_128_SHA`, `TLS_RSA_WITH_RC4_128_MD5`, `SSL_CK_RC4_64_WITH_MD5`.
- **Recommendation:** RC4 has been officially deprecated by RFC 7465 and should not be used.

2. DES (DATA ENCRYPTION STANDARD) AND 3DES (TRIPLE DES)

- **Weaknesses:**
  - **DES:** Uses a 56-bit key, which is now considered too short and vulnerable to brute-force attacks with modern hardware.
  - **3DES:** While an improvement over DES by applying the algorithm three times with different keys, it is significantly slower than modern ciphers and is still vulnerable to certain attacks (e.g., Sweet32 birthday attack) when used in CBC mode with a 64-bit block size.
- **Commonly Found In:** Cipher suites like `TLS_RSA_WITH_3DES_EDE_CBC_SHA`, `SSL_CK_DES_64_WITH_CBC_SHA`, `SSL_CK_3DES_64_WITH_CBC_SHA`.
- **Recommendation:** DES is long obsolete. 3DES is also deprecated for most uses due to performance and potential vulnerabilities, especially when compared to AES.

3. MD5 AND SHA-1 (HASHING ALGORITHMS)

- **Weaknesses:** These are older hashing algorithms that are vulnerable to collision attacks. This means it's feasible for an attacker to find two different inputs that produce the same hash output. While not directly used for encryption, they are often used as part of cipher suites for message integrity or as Pseudo-Random Functions (PRF). Using them in these roles can compromise the security of the entire connection.
- **Commonly Found In:** As part of cipher suites (e.g., `AES256-SHA`, `DHE-RSA-AES128-SHA`) or for certificate signing.
- **Recommendation:** MD5 and SHA-1 should not be used for security-sensitive applications. Modern standards require SHA-256 or stronger hashing algorithms.

4. LOW KEY-STRENGTH CIPHERS

- **Weaknesses:** Ciphers with insufficient key lengths (e.g., historically, 40-bit or 56-bit ciphers) are highly susceptible to brute-force attacks. Even 128-bit ciphers, while generally secure, can be weaker if combined with insecure handshake mechanisms or other vulnerable algorithms.
- **Recommendation:** Prefer ciphers with robust key lengths, such as AES-128 and AES-256.

WHY LEGACY CIPHERS ARE NOT RECOMMENDED ANYMORE

The deprecation of these legacy ciphers is driven by several critical factors:

- **Cryptographic Vulnerabilities:** As mentioned above, these algorithms have known weaknesses that can be exploited by attackers to decrypt traffic, forge messages, or perform man-in-the-middle attacks.
- **Advancements in Computing Power:** What was once computationally infeasible for attackers (like brute-forcing DES) is now achievable.
- **Evolving Security Standards:** Modern security protocols and best practices, such as TLS 1.3, have completely removed support for many of these older, weaker ciphers to ensure a higher baseline level of security.
- **Performance Trade-offs:** While some legacy ciphers might have been faster on older hardware, modern algorithms like AES offer a much better balance of security and performance.

CONCLUSION

Continuing to use legacy OpenSSL ciphers poses a significant security risk. Organizations and individuals should regularly audit their systems and configurations to ensure they are only using modern, strong, and recommended cipher suites. This includes disabling RC4, DES, 3DES, and avoiding the use of MD5 and SHA-1 in security contexts, favouring algorithms like AES, ChaCha20, and SHA-256/SHA-384.

David Keith Jr "mrdj" ✔