The State-of-the-art Cryptographic Algorithms

Kunal Meher[1], Divya Midhunchakkaravarthy[2]

[1]Research Scholar at Lincoln University College, Malaysia and Assistant Professor at Xavier Institute of Engineering, Mumbai.
[2]Associate Professor at Lincoln University College, Malaysia
[1]kunalmeher@gmail.com, [2]divya@lincoln.edu.my

Abstract: *In the paper, the state of the art cryptographic algorithms used in the different popular protocols are discussed. The popular protocols used for secure communication over the Internet are Transport Layer Security (TLS) protocol, Signal protocol, Internet Key Exchange (IKE) protocol, Secure Shell (SSH) protocol and Secure Multipurpose Internet Mail Extensions (S/MIME).*

Keywords: **TLS, IKE, Signal, SSH, S/MIME, AES, ChaCha20, X3DH, Double Ratchet Algorithm**

1. INTRODUCTION

Recently, each communication protocol uses some algorithms to achieve key exchange, confidentiality, authentication, integrity, digital signature. Each of these protocols is released with new versions to keep in line with the state-of-the-art cryptographic algorithms and also remove outdated algorithms.

2. Transport Layer Security (TLS 1.3)

The Transport Layer Security (TLS) protocol is the de facto standard for securing communications on the World Wide Web. It was initially released as Secure Socket Layer (SSL) protocol by Netscape Communications in 1995. Over the years, number of versions of the protocol has been released removing vulnerabilities and making it more secure. Now, it is maintained by the Internet Engineering Task Force (IETF) and current version is TLS 1.3 [1]. Key goals of TLS1.3 are clean up, security, privacy, performance and continuity.

Clean up: TLS 1.3 has removed unsafe, unused features and algorithms from previous versions. TLS 1.3 does not include compression, renegotiation, RSA Key exchange, encryption algorithms - 3DES, Camellia, RC4, hash functions - SHA1, MD5, cipher mode - AES-CBC.

Performance (Faster Speed): The TLS 1.3 handshake process involves only one round-trip as opposed to two in TLS 1.2. This reduces encryption latency by one-half. TLS 1.3 is set to accomplish 0-RTT Resumption. It means that if the client has connected to the server before, TLS 1.3 permits a zero-round trip handshake. With this feature, users will be able to browse websites faster.

Continuity: TLS 1.3 is backward compatible with TLS 1.2. TLS 1.3 clients can communicate with TLS 1.2 servers and TLS 1.2 clients can communicate with TLS 1.3 servers.

Enhanced Security and privacy: TLS 1.3 has removed depreciated features from previous versions. It improves security using modern techniques. It supports Authentication Encryption (AE) scheme. The supported symmetric encryption algorithms are all Authenticated Encryption with Associated Data (AEAD) algorithms. Examples of AE schemes supported are AES-CCM, AES-GCM and ChaCha20-Poly1305. The HMAC-based Extract-and-Expand Key Derivation Function (HKDF) is used as an underlying primitive [2] [3].

TLS 1.2 specifies 37 cipher suites. TLS 1.3 supports 5 cipher suites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256.

TLS 1.3 uses only DHE & ECDHE key exchange algorithms. It supports only 5 ECDHE curve groups and only 5 DHE finite field groups. It has added support for curve 25519 and 448. TLS 1.3 uses RSA PKCS#1 and Edwards-curve Digital Signature Algorithm (ECDSA) / Elliptic Curve Digital Signature Algorithm (EdDSA) digital signature (authentication) algorithms [4].

3. Signal Protocol

The Signal protocol (formally known as the TextSecure Protocol) is a cryptographic messaging protocol that provides end-to-end encryption (E2EE) for instant messaging in Signal, WhatsApp, Wire, Facebook Messenger, Telegram and many others. The Signal Protocol amalgamates the Extended Triple Diffie-Hellman (X3DH) key agreement protocol, Double Ratchet algorithm, pre-keys, and uses Curve25519, AES-256, and HMAC-SHA256 as cryptographic primitives.

The initial key exchange is done using Extended Triple Diffie-Hellman (X3DH) algorithm. X3DH establishes a shared secret key between two parties who mutually authenticate each other based on public keys. X3DH provides forward secrecy and cryptographic deniability [5].

The core of the Signal protocol is Double Ratchet algorithm (Key Management Algorithm). The main idea of Double Ratchet is changing keys for each message. A KDF chain is a core concept in the Double Ratchet algorithm.

A KDF chain (in turn Signal protocol) has the following properties:

- Resilience – adversary can't distinguish keys from random;
- Forward security – if an adversary knows key in a particular moment, he can't find the previous keys;
- Break-in recovery (future secrecy or backward secrecy) – if an adversary knows key in the specific moment, he can't predict future keys [6] [7].

4. Internet Key Exchange (IKEv3)

The Internet Key Exchange is used to generate security associations for the IPsec protocols. IKEv3 makes use of certain cryptographic primitives to achieve its goals of key generation, mutual authentication, and security. AES in SIV mode is used in IKEv3 to accomplish this goal. Synthetic Initialization Vector (SIV) supports authenticated encryption with associated data. IKEv3 defines SHA-256 and SHA-512 for use as hash functions. The IKEv3 uses discrete logarithm cryptography. Authentication can be using public key or PSK. Public key authentication uses a Diffie-Hellman key exchange for key establishment. PSK authentication uses the "dragonfly" key exchange to both generate a shared, and secret, key and to mutually authenticate the peers to each other. [8].

5. Secure Shell (SSHv2)

SSH, or Secure Shell, is an application layer protocol that allows one computer to securely connect to another computer over an unsecured network, like the internet, by having a shared agreement of how to communicate. In SSHv2 protocol, 3DES-CBC is required algorithm; AES128-CBC is recommended and other optional algorithms such as AES256-CBC [9]. SSHv2 currently defines only one key-exchange method, diffie-hellman-group1-sha1. Apart from password authentication SSHv2 provides public key authentication. SSHv2 uses cryptographically strong Message Authentication Code (MAC) algorithms to provide integrity and data origin assurance.

6. Secure / Multipurpose Internet Mail Extension (S/MIME v4.0)

S/MIME is a widely accepted protocol for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them. In S/MIME v4.0 two new encryption algorithms are added namely AES-256 GCM, ChaCha20-Poly1305 and removed AES-192 CBC and 3DES. S/MIME v4.0 added EdDSA and ECDSA algorithms for digital signature and removed DSA. S/MIME v4.0 added SHA-512 as hash function and marked SHA-1 as historic [10].

7. Authenticated Encryption (AE) Scheme

One should never use encryption without providing authentication. The block cipher modes ECB, CBC, OFB, CFB, CTR, and XTS provide confidentiality, but they do not protect against accidental modification or malicious tampering. Examples of AE modes are Counter CBC-MAC (CCM), Galois/Counter Mode (GCM), CWC, EAX, IAPM, and OCB.

7.1 Deterministic Authenticated Encryptions (DAE)

A deterministic encryption scheme (as opposed to a probabilistic encryption scheme) is a cryptosystem which always produces the same ciphertext for a given plaintext and key. Example of DAE cipher is AES-SIV.

7.2 Authenticated Encryption with Associated (Additional) Data (AEAD)

In AEAD, the associated data is used to protect information that needs to be authenticated, but does not need to be kept confidential.
Examples for AE or AEAD ciphers are AES-GCM, AES-CCM and ChaCha20-Poly1305.

8. Resistance to Quantum Computer

The asymmetric parts of such state-of-the art cryptosystems would very likely be exposed to significant risk if we experience a breakthrough in quantum computing in the coming decades. But, Quantum computers able to solve any practical problems more cost-effectively than classical computers are still years away. AES-128 and SHA-256 are both quantum resistant according to the evaluation criteria in the NIST PQC (post quantum cryptography) standardization project. In fact, even a quantum computer capable of breaking RSA-2048 would pose no practical threat to AES-128 whatsoever.

In anticipation of such a quantum computing paradigm, cryptography is being developed and evolved by using so-called “quantum-safe” algorithms. They run on classical computers and are believed to withstand attacks from powerful quantum computers.
When we compare post-quantum cryptography with the currently used asymmetric algorithms, we find that post-quantum cryptography mostly have larger key and signature sizes and require more operations and memory. Still, they are very practical for everything except perhaps very constrained Internet of Things devices and radio [11]. In near future some of the mentioned state-of-the-art cryptographic algorithms will be replaced by their quantum-safe alternatives.

9. Conclusion

In the paper, the popular protocols used in the Internet for secure communication are mentioned such as SSL/TLS, Signal, IKE, SSH and S/MIME. We also mentioned state-of-the-art cryptographic algorithms used in the current version of each of the mentioned protocols such as AE Schemes - AES-CCM, AES-GCM, ChaCha20-Poly1305, Cryptographic Hash Functions - SHA-256, Digital Signature Algorithms - ECDSA/EdDSA, Key Exchange Algorithm - ECDHE (using Curve 25519 or 448), X3DH

and Key Management Algorithm - Double Ratchet algorithm. The two encryption algorithms AES and ChaCha20 are widely accepted. It can be noted that RSA key exchange, DES cryptosystem, SHA-1 and MD5 hash functions are all depreciated. Among the mentioned algorithms ECDSA, EdDSA, ECDHE, X3DH, Double Ratchet algorithm are quantum unsafe while AES, ChaCha20 and SHA-256 are quantum safe.

REFERENCES

[1] *Cas Cremers, Marko Horvat, Jonathan Hoyland, Sam Scott, Thyla van der Merwe, "A Comprehensive Symbolic Analysis of TLS 1.3", CCS'17, pp. 1773-1788.*

[2] *"TLS 1.3 - Enhanced Performance, Hardened Security." [Online]. Available: https://www.cloudflare.com/learning-resources/tls-1-3/.*

[3] *"What You Need to Know About TLS 1.3." [Online]. Available:*

https://www.ssl.com/blogs/need-know-tls-1-3/

[4] *"Overview of TLS v1.3" by OWASP.*

[5] *"The X3DH Key Agreement Protocol." [Online]. Available: https://signal.org/docs/specifications/x3dh/.*

[6] *Julia Bobrysheva, Sergey Zapechnikov, "Post-Quantum Security of Messaging Protocols: Analysis of Double Ratcheting Algorithm", IEEE, 2020, pp. 2041 – 2044.*

[7] *"The Double Ratchet Algorithm." [Online]. Available: https://signal.org/docs/specifications/doubleratchet/.*

[8] *"The (Real) Internet Key Exchange." [Online]. Available: https://tools.ietf.org/html/draft-harkins-ikev3-00.*

[9] *"The Secure Shell (SSH) Transport Layer Protocol." [Online]. Available: https://tools.ietf.org/html/rfc4253.*

[10] *"Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification." [Online]. Available: https://tools.ietf.org/html/rfc8551.*

[11] *"What next in the world of post-quantum cryptography?" [Online]. Available: https://www.ericsson.com/en/blog/2020/3/post-quantum-cryptography-symmetric-asymmetric-algorithms.*