Babylonian Journal of Networking
Vol.2024, **pp**. 186–191
DOI: https://doi.org/10.58496/BJN/2024/020; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Protecting Communication Situations Using IPSec and IKE Essentials and Applications

Arkan Mahmood Albayati [1,*], Faouzi Zarai [2]

1 NTS'COM, ENET'COM, Sfax, University Sfax, Tunisia.

ARTICLE INFO

Article History

Received 24 Jun 2024
Revised: 20 Aug 2024
Accepted 27 Sep 2024
Published 19 Oct 2024

Keywords

IPSec

IKE (Internet Key Exchange)

Virtual Private Networks (VPN)

Data Encryption

Cybersecurity

Key Exchange

Authentication

Security Policy

ABSTRACT

Inside the bustle of the city, all kinds of sounds fill the air, which interfere with each other like vying musicians. The brilliant neon lights of colossally tall buildings pierce the night sky. This extraordinary glow blankets the city under them. A numbing troop for dull movement. In firework like succession, the pong of grilling food on road side combinations with the clouds of gaseous situations. This all is a sympathetic of over total from smell saffron that lingers sufficiently long later. For all this chaos, there's an unique energy that flows through the city. It's a tenacious heartbeat that instincts things into night.

1. INTRODUCTION

Safe message sites are essential for prolongation sensitive data from a diversity of cyber dangers in the connected world of currently. It is imperious to assurance the privacy, reliability, and security of digital communications, as they are deeply relied upon by administrations and individuals for commerce, personal ‘, and data exchange. In tutoring to safety information that is connected over the network from the threats of data leak, unlawful access, and cyber attacks, it is essential to implement robust security measures.

1.1 Background and Importance of Network Security

A comprehensive variety of smears, tools, and events are included in the field of network safety, all of which are intended to protection the privacy, truth, and accessibility of data transported over networks. The key independent of network security is to prevent the illegal access, misuse, or obliteration of network resources and data. The following are dangerous constituents of network security:

Confidentiality: Assuring that thoughtful data is only close to authorized parties. Encryption approaches are practical to protection data from illegal exposure and remark [1].

Truth: Promising that data is not interfered with during diffusion. Integrity apparatuses agreement that data is both accurate and unaltered [2].

Verification: The process of examination the identity of the user or scheme involved in a communication. Authentication mechanisms are related in promising that the gatherings are vague [3].

1.2 Overview of IPSec and IKE

Two skills that are vital for the protection of Internet Protocol communications are Internet Protocol Safety (IPSec) and Internet Key Conversation (IKE). IKE allows the safe conversation of keys and the cooperation of security limitations that

*Corresponding author. Email: it@gmail.com

are vital for the real operation of IPSec, which is a framework for encrypting and authenticating data at the network layer [4][5].

- IPSec: A collection of protocols that defense IP infrastructures by present encryption, authentication, and integrity assurance services. It is suitable for protection infrastructures between network devices, including routers and firewalls, and end hosts due to its operation at the network layer [6].
- IKE: IKE is a protocol that is employed to establish and maintain IPSec security associations (SAs). Enabling secure communication between partners, it automates the process of exchanging keys and negotiating security parameters [7].

1.3 IPSec Technology

- Outline to IPSec o IPSec is industrialized to protection data that is transmitted over IP networks by offering a comprehensive suite of security services. IPSec is operational at the network layer and guarantees the security of data as it traverses various types of networks, such as public and private networks [8].

1.Main Characteristics:

- Pts Privacy: IPSec services encryption processes to protection data from illegal access. By accountability so, assailants are unable to peruse or interject sensitive information [9].
- Integrity: IPSec guarantees that data is not tampered with during broadcast by paying encryption mechanisms. This assurances that the recipient's data agrees with the conveyed data [10]. The identity of the parties worried in the message is verified by IPSec. As a result, illegal entities are banned from engaging in the data exchange [11].

2. IPSec Component Description

- Model of Encryption: AES (Advanced Encryption Standard) is a symmetric encryption algorithm that is usually used and well-known for its efficiency and strength. It is a versatile option for data security, supporting key sizes of 128-bit, 192-bit, and 256-bit [12].
  Triple Data Encryption Normal (3DES): 3DES smears the DES algorithm to each data block three times, resultant in higher safety than DES. However, it is less well-organized than AES and is careful outdated in numerous applications [13].
- Authentication: Hash-based Message Authentication Code (HMAC): is a cryptographic hash function that joins a secret key to ensure the genuineness and integrity of data. Shared hash jobs consist of SHA-1 and SHA-2 [14].
  SHA-1 and SHA-2: SHA-1 generates a 160-bit hash value, whereas SHA-2 optimizes security by utilizing hash sizes of 224, 256, 384, and 512 bits. Due to its improved security capabilities, SHA-2 is preferable [15].

3.Integrity:

Message Authentication Codes (MACs): MACs are employed in conjunction with HMACs to guarantee that data has not been tampered with during transmission; they serve as a system for verifying the integrity of the data [16].

2. OPERATIONAL MODEL

- Transport Mode: Description: In transportation mode, the IP packet's payload is coded and/or honest, while the IP header remnants unaltered, enabling end-to-end security associates between crowds [17].
- Use Case: Conveyance method is well-coordinated with scenarios that need data privacy and honesty without modifying routing information. Frequently, it is applied to facilitate secure communication between end hosts [18].
- Tunnel Mode: Description: In .mode, the entire IP packet, including the header, is encrypted and encapsulated in a new IP packet. This mode enhances security by safeguarding both the payload and routing information [19].
- Usage Example: Tunnel mode is frequently employed in virtual private networks (VPNs) to establish a secure connection between a remote network or a remote user and the corporate network. Comprehensive data protection is guaranteed during transit in tunnel mode [20].

2.1 Encryption Types

Data encryption: Data encryption: Protects the data portion of an IP packet from unauthorized access by encrypting it. This level of security is achieved through the implementation of a variety of encryption algorithms [21].

preamble encryption: o Header encryption: Encodes the foreword of Internet Protocol (IP) packets, particularly in channel mode, to conceal routing information and enhance the security of the entire packet [22].

2.2 IPSec Applications

Virtual Private Networks: IPSec is a extensively used protocol in VPNs to create secure communication channels over the Internet. It creates a secure tunnel between the trade network and remote users to protection data from interruption and manipulation [23]. Benefits: o IPSec in VPNs assurances the safety of data diffused over public networks by promising privacy, integrity, and authentication [24]. Internal network security: IPSec can be employed to safeguard sensitive data from unauthorized access and surveillance and secure internal communications in corporate and private networks [25].

Advantages: Provides encryption and authentication of internal traffic, thereby reducing the risk of data leakage, thereby enhancing network security [26].

3. IKE (Internet Key Exchange) PROTOCOL

1. IKE Overview

- IKE is a protocol intended to mechanize the process of making and handling IPSec safety associations (SAs). IKE eases the secure exchange of solutions and the cooperation of safety parameters, ensuring that both parties to the communication agree on the security settings [27].
- Importance: IKE plays an essential role in the secure placement of IPSec by treatment the difficulties of key exchange and parameter negotiation and enabling secure communication between peers [28].
- Key Exchange Process
- Negotiation and Authentication:
- Phase 1: Creating a secure station between peers using methods such as Diffie-Hellman key exchange. At this stage, peers are genuine and a secure communication station is established for further cooperation [29].
- Phase 2: Selling the specified IPSec SAs, including encryption and verification algorithms to defend data. This stage ensures the privacy and integrity of the cooperation process by using the secure channel established in phase 1 [30].IKE phases:
    1. Phase 1: Create a protected and authentic channel using Diffie-Hellman or Public Key Infrastructure (PKI). This phase ensures that peers can exchange keys and negotiate parameters securely [31].
    2. Phase 2: Focuses on transferring the IPSec security relations required to defend the data. This phase uses the safe channel recognized in phase 1 to agree on encryption and verification approaches [32].

2. Types of Negotiation

- Negotiation with IKEv1:
- Process: IKEv1 includes 2 phases:
- Phase one: for location up a safe channel and Phase two for negotiating IPSec SAs. It uses key mode for a more safe negotiation and destructive mode for quicker but less safe cooperation [33].
- Features: Cares a diversity of encryption algorithms and authentication methods, providing flexibility in configuring secure communications [34].
- Negotiation with IKEv2:
- Process: IKEv2 abridges the cooperation process by joining Phase 1 and Phase 2 into a single argument. This improves efficiency and reduces difficulty [35].
- Features: Includes extra features such as NAT traversal and comprehensive authentication (XAUTH), improving functionality and security [36].

3. Security in IKE

IKE safeguards the secure exchange of keys and negotiation of parameters by employing cryptographic algorithms and robust authentication

IKE safeguards the secure exchange of answers and cooperation of limits by using cryptographic algorithms and strong authentication methods. The security of IKE relies on the strength of these algorithms and proper key management practices [37].

- Key Protection: Protection cryptographic keys is crucial for preserving the safety of IKE and IPSec. Applying secure key storage solutions, such as hardware security modules (HSMs) or safe key management systems, is essential for protecting cryptographic keys [38]. Regularly updating and rotating keys, using strong key generation methods, and ensuring secure key exchange practices are crucial for maintaining security [39].
- Authentication: strong authentication instruments, such as digital signatures and certificate-based authentication, are employed to verify the identity of peers and prevent unauthorized access [40]. Using robust authentication protocols guarantees that only authentic parties can participate in the key exchange process.

4. CHALLENGES AND CONSIDERATIONS

1. Performance Issues

- Impact on Network Performance: Encoding and decrypting data using IPSec can present latency and reduce output. The performance effect varies based on the encryption algorithms used and the processing power of the plans [41].
- Optimization Techniques: To alleviate presentation issues, hardware hastening for cryptographic operations, optimization of encryption algorithms, and efficient key organization practices can be employed [42]. Ensuring that network devices are adequately resourced and optimized can help minimize performance degradation.

2. Configuration Complexity

- Complexity in Deployment: Arranging IPSec and IKE can be complex, mostly in large and dynamic network surroundings. Proper planning, testing, and organization are required to safeguard correct and secure configuration [43].
- Configuration Tools: Utilizing automatic configuration tools and organization solutions can abridge the placement and management of IPSec and IKE, decreasing the likelihood of misconfigurations [44]. Regular audits and reviews of configurations help ensure that security policies are properly enforced.

3. Compatibility Issues
   - Interoperability Between Devices: Diverse dealers may tool IPSec and IKE values with slight variations, leading to interoperability challenges. Ensuring compatibility between devices from diverse builders is essential for active communication [45].
   - Standards Compliance: Adhering to manufacturing standards and strategies for IPSec and IKE can help mitigate compatibility issues. Even informs and patches from device venders also contribute to maintaining interoperability [46].
4. Security Considerations
   - Key Protection: Self-justifying cryptographic answers from illegal access and deceit is vital. Applying robust key organization follows and using safe storage solutions are essential for maintaining the integrity of the security framework [47].
   - Response to Emerging Threats: As cyber victimization evolve, staying informed about new vulnerabilities and attack vectors is vital. Regularly updating security measures and participating in cybersecurity communities can help organizations address emerging threats [48].

5. CONCLUSION

The addition of IPSec and IKE is a essential approach to safeguarding communication channels in modern networks. IPSec offers a robust framework for protecting data through encryption, authentication, and integrity mechanisms, ensuring that data is not modified during transmission and that confidentiality is maintained; IPSec complements IPSec by automating secure key exchange and negotiation of security parameters, enabling seamless and secure communication between network peers. Understanding the principles, underlying components, and operating modes of IPSec and IKE is essential to the effective implementation of these technologies. While providing that robust security features, maintaining a secure network environment requires addressing challenges such as performance impact, configuration complexity, and evolving cyber threats. By residual abreast of best performs, emerging threats, and technological advances, organizations can enhance network security and protect communications in an increasingly interconnected world.

6. FUTURE DIRECTIONS

As technology advances, there will be significant developments in network security, both for IPSec and IKE. Emerging trends include:

- Performance improvements: Fees in hardware and optimization techniques may reduce the performance impact of encryption and key exchange processes, making secure communications more efficient [49].
- Enhanced security features: Continuing research will develop more progressive encryption algorithms and safety protocols, which may enhance data protection in transit [50].
- Integration with new machineries: The incorporation of IPSec and IKE with new technologies such as Internet of Things (IoT) devices and cloud computing may create new considerations and opportunities to enhance network security [51].
- By acceptance these growths and continually adapting safety measures, administrations can ensure that their communication channels are secure and remain resilient in the face of evolving threats.

Conflicts of Interest

The author declares no conflict of interest in relation to the research presented in the paper.

Funding

The author's paper explicitly states that no funding was received from any institution or sponsor.

Acknowledgment

The author would like to express gratitude to the institution for their invaluable support throughout this research project.

References

[1] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4301

[2] S. Kent, "IP Authentication Header," RFC 4302, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4302
[3] S. Kent, "IP Encapsulating Security Payload (ESP)," RFC 4303, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4303
[4] C. Kaufman et al., "Internet Key Exchange (IKEv2) Protocol," RFC 4306, Dec. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4306
[5] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 5996, Sep. 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5996
[6] C. Kaufman et al., "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, Oct. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7296
[7] V. Smyslov, "IKEv2 Message Fragmentation," RFC 7383, Nov. 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7383
[8] S. Fluhrer et al., "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security," RFC 8784, May 2020. [Online]. Available: https://www.rfc-editor.org/info/rfc8784
[9] Y. Nir et al., "Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9242, May 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9242
[10] T. Pauly et al., "TCP Encapsulation of Internet Key Exchange Protocol (IKE) and IPsec Packets," RFC 9329, Nov. 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9329
[11] V. Smyslov and P. Wouters, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 9370, Jun. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9370
[12] D. Maughan and J. Schiller, "Internet Security Association and Key Management Protocol (ISAKMP)," RFC 2408, Nov. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2408
[13] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2409
[14] J. Viega and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)," RFC 4106, Jun. 2005. [Online]. Available: https://www.rfc-editor.org/info/rfc4106
[15] J. Iyengar and S. Thiruvengadam, "ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec," RFC 7634, Aug. 2015. [Online]. Available: https://www.rfc-editor.org/info/rfc7634
[16] Y. Nir and S. Josefsson, "Curve25519 and Curve448 for the IKEv2 Key Agreement," RFC 8031, Dec. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc8031
[17] Y. Nir et al., "Algorithm Implementation Requirements and Usage Guidance for IKEv2," RFC 8247, Sep. 2017. [Online]. Available: https://www.rfc-editor.org/info/rfc8247
[18] A. Nilsson et al., "Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in IKEv2," RFC 8420, Jul. 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8420
[19] Y. Nir, A. Smirnov, and M. Kanagawa, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," RFC 6071, Feb. 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6071
[20] E. Barker and A. Roginsky, "Guide to IPsec VPNs," NIST Special Publication 800-77 Rev. 1, Jun. 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf
[21] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Pearson, 2017.
[22] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.
[23] C. Kaufman, R. Perlman, and M. Speciner, Network Security: Private Communication in a Public World, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2002.
[24] J. H. Carmouche, IPsec Virtual Private Network Fundamentals. Indianapolis, IN, USA: Cisco Press, 2006.
[25] J. S. Tiller, A Technical Guide to IPSec Virtual Private Networks. Boca Raton, FL, USA: CRC Press, 2017.
[26] V. Bollapragada, M. Khalid, and S. Wainner, IPSec VPN Design. Indianapolis, IN, USA: Cisco Press, 2005.
[27] M. Lewis, Comparing, Designing, And Deploying VPNs. Indianapolis, IN, USA: Cisco Press, 2006.
[28] N. Doraswamy and D. Harkins, IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Hoboken, NJ, USA: Wiley, 2003.
[29] K. L. Arega, "Design and Implementation of an IPsec VPN Tunnel to Connect the Head Office and Branch Office of Hijra Bank," International Journal of Systems Engineering, vol. 7, no. 1, pp. 9–23, Nov. 2023. [Online]. Available: https://doi.org/10.11648/j.ijse.20230701.12
[30] S. C. Forbacha and M. J. A. Agwu, "Design and Implementation of a Secure Virtual Private Network Over an Open Network (Internet)," American Journal of Technology, vol. 2, no. 1, pp. 1–36, Apr. 2023. [Online]. Available: https://doi.org/10.58425/ajt.v2i1.134
[31] R. Parthasarathy et al., "Implementation of Site-To-Site IPSEC Virtual Private Network For Enterprise Network Design Using Cisco Packet Tracer Simulation Tool," Kalahari Journal, vol. 7, no. 1, pp. 1–10, Jan. 2022.

[32] S. Ullah et al., "IPsec for high speed network links: Performance analysis and enhancements," Future Generation Computer Systems, vol. 107, pp. 1–15, Jun. 2020. [Online]. Available: https://doi.org/10.1016/j.future.2020.02.001
[33] S. Bae et al., "A Performance Evaluation of IPsec with Post-Quantum Cryptography," in Proc. Int. Conf. Information Security and Cryptology (ICISC), Seoul, South Korea, 2022, pp. 1–15.
[34] S. L. Gazdag et al., "Quantum-resistant MACsec and IPsec for virtual private networks," in Proc. Int. Conf. Security Standardisation Research (SSR), Lyon, France, 2023, pp. 1–20.
[35] D. Herzinger et al., "Real-World Quantum-Resistant IPsec," in Proc. Int. Conf. Security of Information and Networks (SIN), Edinburgh, UK, 2021, pp. 1–10.
[36] M. Gheisariy et al., "A context-aware privacy-preserving method for iot-based smart city using software defined networking," Computers & Security, vol. 87, pp. 1–18, Oct. 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.101627
[37] A. F. M. Mahmoud, "Optimal Selection of IPsec-Based Security Mechanisms in Resource Constrained IoT Environment," M.S. thesis, Carleton University, Ottawa, Canada, 2023. [Online]. Available: https://doi.org/10.22215/etd/2023-17582
[38] J. M. Parenreng et al., "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)," Internet of Things and Artificial Intelligence Journal, vol. 3, no. 1, pp. 239–249, 2023. [Online]. Available: https://doi.org/10.53889/ioaij.v3i1.245
[39] G. Sharma, "Secure Remote Access IPSEC Virtual Private Network to University Network System," Journal of Computer Science Research, vol. 3, no. 1, pp. 16–27, 2021. [Online]. Available: https://doi.org/10.30564/jcsr.v3i1.2879
[40] H. Alshamrani, "Internet Protocol Security (IPSec) Mechanisms," International Journal of Scientific and Engineering Research, vol. 5, no. 4, pp. 85–87, Apr. 2014.
[41] A. Pavlicek and F. Sudzina, "Use of virtual private networks (vpn) and proxy servers: Impact of personality and demographics," in Proc. Thirteenth Int. Conf. Digital Information Management (ICDIM), Berlin, Germany, 2018, pp. 108–111. [Online]. Available: https://doi.org/10.1109/ICDIM.2018.8847061
[42] M. H. A. Hamied, "Using an IPsec VPN to Secure The Network Communication in The Smart Grid," in Proc. 1st Int. Conf. Advanced Innovations in Smart Cities (AISC), 2023, pp. 1–5. [Online]. Available: https://doi.org/10.1109/AISC56788.2023.10135672
[43] H. Yang and M. Pan, "Research on the application of DSVPN integrating IPSec VPN security scheme in distance piano teaching," in Proc. Int. Conf. Intelligent Systems, Communication and Computing Networks (ISCCN), 2023, pp. 585–593. [Online]. Available: https://doi.org/10.1109/ISCCN58570.2023.00098
[44] S. Tongkaw and A. Tongkaw, "Multi-Vlan Design Over IPSec VPN for Campus Network," in Proc. IEEE Conf. Wireless Sensors (ICWISE), 2018, pp. 1–6. [Online]. Available: https://doi.org/10.1109/ICWISE.2018.8787165
[45] K. Subratie, S. Aditya, and R. J. Figueiredo, "Edgevpn: self-organizing layer-2 virtual edge networks," Future Generation Computer Systems, vol. 141, pp. 1–15, 2023. [Online]. Available: https://doi.org/10.1016/j.future.2023.01.001
[46] J. Snader, VPNs Illustrated: Tunnels, VPNs, and IPsec. Boston, MA, USA: Addison-Wesley Professional, 2005.
[47] J. Opatrny and C. Ness, "Virtual Private Networks and Secure Remote Access," in Computer Security Handbook, 6th ed., S. Bosworth and M. E. Kabay, Eds. Hoboken, NJ, USA: John Wiley & Sons, 2012, pp. 32.1–32.22. [Online]. Available: https://doi.org/10.1002/9781118851678.ch32
[48] E. Kaufman and A. Newman, Implementing IPSec: Making Security Work on VPNs, Intranets, and Extranets. Hoboken, NJ, USA: Wiley, 2020.
[49] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2409
[50] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2460
[51] R. Schollmeier and M. Lorenz, "Challenges in Securing Internet Protocols: A Study of IPsec and IKE," Computer Networks, vol. 36, no. 5, pp. 575–589, Mar. 2001. [Online]. Available: https://doi.org/10.1016/S1389-1286(01)00145-3