Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2605684, 7 pages
https://doi.org/10.1155/2022/2605684

Research Article

Detecting IKEv1 Man-in-the-Middle Attack with Message-RTT Analysis

Yunxiao Sun,[1] **Bailing Wang**,[1] **Hongri Liu**,[1] **Yuliang Wei**,[1] **Di Wu**,[2] **and Jing Wang**[3]

[1]*Harbin Institute of Technology, 264209 Weihai, China*
[2]*School of Computer Science of Beijing University of Posts and Telecommunications, 100876 Beijing, China*
[3]*Information Research Center of Tsinghua University, 100084 Beijing, China*

Correspondence should be addressed to Bailing Wang; wbl@hit.edu.cn

Received 31 March 2022; Revised 18 May 2022; Accepted 23 May 2022; Published 14 June 2022

Academic Editor: Junjuan Xia

The IPSec has been a widely used VPN (virtual private network) protocol due to its security and convenience. The security of IPsec itself plays a fundamental role in the overall security of the application system. However, it can be found from the existing research that because of some insecurity issues in the application process, the IPsec protocol will suffer from the man-in-the-middle attack. In this paper, we constructed the first experiment environment of IKE (Internet Key Exchange) man-in-the-middle detecting, use normal distribution to detect the RTT (round-trip time), and get 90% of accuracy.

1. Introduction

IPsec is a secure network protocol suite that authenticates and encrypts network packets to allow safe encrypted communication between two computers over an Internet protocol network [1]. IPSec is a commonly used protocol for building VPN (virtual private network) tunnels that provide security for VPN negotiations and network access to random hosts. IKE (Internet Key Exchange) is a key management protocol that is used in conjunction with the IPSec protocol. It is a way of sharing encryption and authentication keys over an insecure channel. The IKE functions work in two stages: (1) creates an authenticated communication channel between peers by employing methods such as the Diffie-Hellman key exchange, which provides a shared key that is used to further encrypt IKE conversations; (2) the peers use the secure communication channel to negotiate security on behalf of other services such as IPSec. These methods result in the creation of two unidirectional channels, one inbound and the other outgoing.

Various security protocols have developed methods to protect against man-in-the-middle attacks over time. Asymmetric key agreement technology is used in all mainstream security protocols, including TLS, SSH, and IKE. The man-in-the-middle attacks can disrupt the key exchange process by replacing both parties' public keys. As a result, identity authentication is incorporated into security protocols. Different techniques of attacking the IPSec protocol have been documented in the literature [2–4], and man-in-the-middle attacks have always been a major threat source for security protocols [5]. Wireless networks, local area networks, and even wide-area networks are all vulnerable to man-in-the-middle attacks. Users may or may not have a clear perception when an attack happens.

The man-in-the-middle attack detection method is also distinct from methods used in typical intrusion detect systems [6]. Man-in-the-middle attacks have a better level of concealment than typical network attack methods like SQL injection and remote code execution. The network traffic was indistinguishable from normal traffic at the time of the attack. Man-in-the-middle attacks are impossible to protect against with firewalls and intrusion detection systems. Mirsky et al. [7] designed a man-in-the-middle attack detection algorithm named Vesper, which can identify man-in-the-middle attacks in LAN networks by measuring the RTT of echo packets. However, this method cannot detect attacks against specific application protocols and is difficult to apply to the WAN environment. According to current research, the IKE protocol is widely used, but there are also various attacks against the protocol. If the user selects the preshared key authentication mode, when a man-in-the-middle attack occurs, neither the client nor the server can perceive the existence of the attack. Therefore, it has become an important task to study how to detect man-in-the-middle attacks in the IKE communication process. This paper provides a calculating approach based on RTT delay to detect whether there is a man-in-the-middle in the communication process to check and prevent the existence of man-in-the-middle attacks in the IPsec application process.

Our main contributions are as follows: (1) built the experimental environment for the IKE man-in-the-middle attack; (2) analyzed the statistical properties of RTT and concluded that RTT conforms to a normal distribution; (3) proposed a man-in-the-middle attack detection algorithm for IKE based on the confidential intervals of normal distribution, which achieved 90% accuracy rate; and (4) found the problem of unintentional leakage of the preshared key through case study. Compared with the existing methods, our proposed algorithm is nonintrusive to the system, only uses network traffic, and does not need to change the IPSec software source code and network topology. The algorithm has certain versatility and may be integrated into the intrusion detection system or applied to the man-in-the-middle attack detection of other security protocols.

2. Background Knowledge

The MITM attacker's ability is the Dolev-Yao model. The attacker can modify or delete message from the network. The middle-man model is based on the Dolev-Yao model. The main capabilities include the following:

(i) Familiar with modern cryptography. The attacker can decrypt the message with the right key

(ii) Familiar with the protocol and know the entities involved in the protocol

(iii) Has complete control over the network and can eavesdrop and intercept any messages transmitted in the system

In IKEv1, the main mode is an instantiation of the ISAKMP (Internet Security Association Key Management Protocol) identity protect exchange: the first two messages negotiate policy; the next two exchange Diffie-Hellman public values and ancillary data (e.g., nonces) necessary for the exchange; and the last two messages authenticate the Diffie-Hellman exchange. The authentication method negotiated as part of the initial ISAKMP exchange influences the composition of the payloads but not their purpose. The result of either main mode or aggressive mode is three groups of authenticated keying material shown in equations (1)–(4). The $N_i$and N_r are the nonces generated by the initiator and the responder separately. The x and y are the Diffie-Hellman public key of the peers, which are known as key exchange payload in the IKE message. The CKY_i and CKY_r are the SPI (Security Parameter Index) in the IKE message. The function PRF means pseudorandom function, which is used as the algorithm to derive key materials. SKEYID is the key seed, SKYEID_*e* is the key material used by ISAKMP SA to protect the confidentiality of its messages, SKYEID_*a* is the key material that ISAKMP SA uses to authenticate its messages, and SKYEID_*d* is the key material used to derive keys for non-ISAKMP SA.

$$\mathrm{SKEYID} = \mathrm{PRF}(\mathit{pre\_shared\_key}, N_i|N_r), \tag{1}$$

$$\mathrm{SKYEID\_}d = \mathrm{PRF}(\mathrm{SKEYID}, g^{xy}, \mathrm{CKY}_i|\mathrm{CKY}_r|0), \tag{2}$$

$$\mathrm{SKYEID\_}a = \mathrm{PRF}(\mathrm{SKEYID}, \mathrm{SKYEID\_}d, g^{xy}, \mathrm{CKY}_i|\mathrm{CKY}_{\mathrm{r}}|1), \tag{3}$$

$$\mathrm{SKYEID\_}e = \mathrm{PRF}(\mathrm{SKEYID}, \mathrm{SKYEID\_}a, g^{xy}, \mathrm{CKY}_i|\mathrm{CKY}_r|2). \tag{4}$$

Because Diffie-Hellman is vulnerable to man-in-the-middle attacks, IKE introduced an identity authentication mechanism to prevent man-in-the-middle attacks during key exchange. IKEv1's identity authentication mechanism includes four types: two RSA-based methods, a digital signature-based method, and a preshared key-based method. The first three methods require the IPSec network administrator to issue a certificate for the user, and the user imports the certificate on their client device. The preshared key method requires the IPSec administrator to set a string password and send the string password to the user for configuration. The preshared key method is easy to operate and widely used. This type of authentication method is commonly used for VPN services for sale, and it is also used by many colleges and enterprises. Because users and network administrators do not have a deep understanding of the IPSec protocol, it is generally believed that the username and password used for login are required to be kept secret, and the preshared key does not need to be kept secret.

Through the analysis of the IKE key derivation process, when the man-in-the-middle attacker obtains the PSK, he can calculate the communication key with the client and the server, respectively, which shown in Figure 1.

The attacker controls the communication link between the initiator and the responder and can forward network packets and modify the content of the packets. In the message exchange process of the IKE protocol, the initiator first sends its SA proposal to the responder, and the responder selects the optimal combination of cryptographic algorithms from the SA proposal according to a certain security policy. At this stage, the attacker needs to parse the information necessary for the man-in-the-middle attack from the received message and forward the message without modifying the message content. In the second pair of messages, the initiator and the responder need to exchange the Diffie-Hellman public key and the nonce for the calculation of the key material. The attacker needs to generate two pair of Diffie-Hellman keys, including the public keys and the private keys, replace the initiator's public key ke_i with his own public key $\mathrm{fake\_ke}_i$, and replace the responder's public key ke_r with his own public key $\mathrm{fake\_ke}_r$. After the public key replacement is completed, the attacker can negotiate key material with the initiator and responder separately by

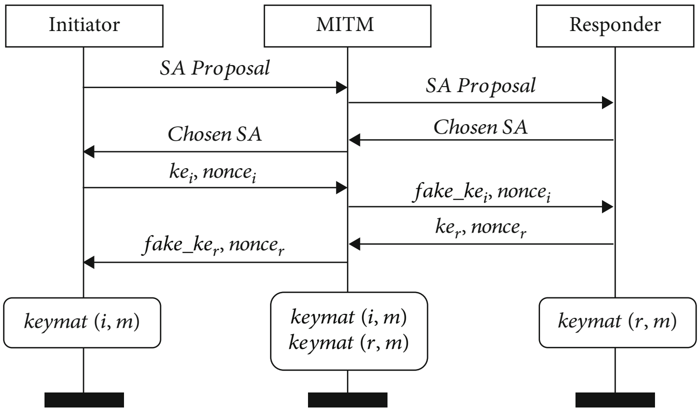

Figure 1: The man-in-the-middle attack of IKE.

the function keymat, thereby destroying the confidentiality and data integrity of the communication. Different from the traditional intrusion detection technology, man-in-the-middle attack detection does not have obvious characteristics. The network data message attacked by man-in-the-middle is the same as that under normal conditions in terms of length, contracting frequency, and so on. IPSec packets are encrypted; it is impossible to identify whether there is an intermediary in the link through the communication content. This brings challenges to man-in-the-middle attack detection.

Because the operation of Diffie-Hellman algorithm involves large number operation, the CPU time consumed cannot be masked by network jitter. Theoretically, when there is man-in-the-middle attack, on the client side, the round-trip time of the second pair of messages in IKE protocol will be significantly longer than that under normal circumstances. Therefore, this paper attempts to analyze the time consumed by each message interaction in the running process of IKE protocol to judge whether there are exceptions in the process of negotiation interaction.

3. The Problem Definition and Solution

3.1. MPRTT Definition. Protocol in C-S model, the client is the initiator, and the server is the responder. The message sequence of client denoted as $M_{cs} = \{m_{c1}, m_{c2}, \cdots, m_{\text{cn}}\}$, while the message sequence of server denoted as $M_{sc} = \{ m_{s1}, m_{s2}, \cdots, m_{sn}\}$.

To start a new session, the client needs to do some initial operation including nonce generation, key generation, and cipher suite choice and then send out the first message m_{c1} over the network channel. The server will respond a message m_{s1} after processing the client's message.

Definition 1. A message pair means the initial message m_{cn} and its corresponding response message m_{sn}, donated as $MP_n = <m_{sn}, m_{cn} >$.

Definition 2. MPRTT_n denotes the time cost of processing the n-th message pair, and T_{cn} is the timestamp that client send the message m_{cn}, while T_{sn} is the timestamp that client receive the message $m_{sn}$from server. RTT is the round-trip time cost of a pair of messages. Then, $MPRTT_n = T_{sn} - T_{cn}$. The measurement method of MPRTT_n is shown in Figure 2.

The MPRTT_n represents the time spent by the client to process a pair of protocol messages, including fixed event delay and random event delay in the communication process. Fixed event delay is the sum of network channel transmission delay and protocol message processing delay in an ideal environment; random events include delays caused by events such as router queue cache, operating system cache, and operating system thread scheduling. In an ideal environment, the network channel transmission delay is recorded as $\text{COST}_{\text{chan}}$, the protocol message processing delay is recorded as $\text{COST}_{\text{proto}}$, and the delay caused by random events in the communication process is recorded as $\text{COST}_{\text{jitter}}$.

Definition 3. ΔRTT is the difference between the n-th message RTT and the RTT of the next message that means $\Delta \text{RTT}_n = \text{MPRTT}_{n+1} - \text{MPRTT}_n$. For a certain system with IPSec device, ΔRTT is a variable with jitters, and it is a normal distribution. The ΔRTT with MITM attack is different from a normal system. The MITM detection problem can be transformed to a ΔRTT abnormal detection problem. Our approach of abnormal detection is based on the confidence interval of normal distribution.

3.2. ΔRTT Distribution. We studied the distribution of ΔRTT using statistic methods. The Grubbs method is to delete the outliners from the samples. There are three modes: left, right, and two-tailed. According to the experiments result, in two-tailed mode, the result is the best. Figure 3 shows the result after deleting the outliner data with Grubbs method. With the shape of Figure 3 and the quantile-quantile plot shown in Figure 4, we can assume that the ΔRTT is according with normal distribution.

3.3. ΔRTT Abnormal Detection. The main idea of detection algorithm is anomaly detection based on normal distribution confidence interval. The experimental data includes two parts: training set and test set. The training set has only

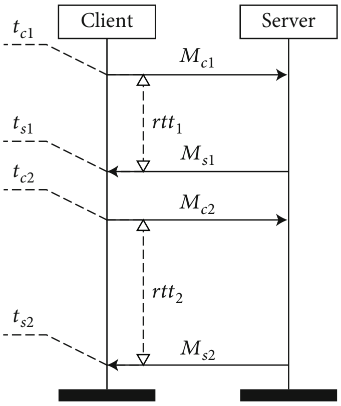

Figure 2: The measurement of MPRTT.

positive samples, that is, ΔRTT measurements under normal conditions. The anomaly detection algorithm is divided into three steps.

(1) Through the fitting of normal distribution, we can calculate the mean value μ and standard deviation σ of the samples

(2) Under a certain significance level α, calculate the confidence interval $[C_1, C_2]$

(3) For the ΔRTT value X measured in one IKE session, if $C_1 \leq X \leq C_1$, the X is normal and there is no man-in-the-middle attack. Otherwise, the X will be considered as abnormal, and there may exists a man-in-the-middle attacker over the channel

4. Experiments

4.1. Experiments Environment. The network topology of the experimental environment is shown in Figure 5. The IKE client runs on Windows 10 and macOS 10.15, respectively, using the built-in client software of the operating system. The IKE server runs on Alibaba cloud ECS, and the operating system is CentOS 7 2. The server software version is libreswan 1.39. The device *MITMBox* is the man-in-the-middle attacker, and the software is built based on several open-source software including DPDK, libgcrypt, and OpenSSL.

4.2. Data Sets. We implemented the attack program according to the IKE man-in-the-middle attack method mentioned in the paper of G. Wang et al. [8]. We implemented a IKEv1 MITM device; the device can forward the packet using DPDK. The result shows that with a known preshared key, we can break the Diffie-Hellman process in IKEv1 session and calculate a pair of keys between the initiator and responder. Then, we can break the secrecy and the authentication of ESP; packets transported in IPSec tunnel can be decrypted to plaintext.

We also implemented an automated tool to calculate the RTT of the IKE messages. The timestamp of a packet in *libpcap* is recorded in pcap frame header. In libnids, we use *nids_last_pcap_header* to get the pcap header, and *ts* in pcap header structure is the timestamp of current message, which is being processed in the callback function. The structure is defined in *nids.h* and *pcap.h*. The timestamp of each message is stored in an array, one array for M_{cs} and one for M_{sc}. The data measured for each IKE connection is taken as one sample, and the average value of three consecutive sampling results is taken as the RTT measurement result.

The automate tools support different operating systems. For Windows, we use *radialup* to connect IKE server. For macOS, we use *network-setup* to connect an IKE connection. And on Linux, we use *network-manager* to connect the IKE server. All the connect task can be managed with script programming language, such as shell and powershell. MPRTT measuring method is based on deep packet inspection. There are several open-source tools to capture packet during IKE session on client side. *tcpdump* or *dumpcap* are command line tools, and they are easy to make a automate packet capture engine, with the help of bash on Linux, or *powershell* on windows. The tools save the message in pcap format.

4.3. Experiment Results. The metrics utilized in classification tasks are used to evaluate our technique in this study. When an attack class is used as a positive class, for example, four different types of classification results are displayed below.

(i) True Positive (TP). There exists MITM attack and the classifier marked this sample as abnormal

(ii) False Positive (FP). There is no MITM attack and the classifier marked this sample as abnormal

(iii) True Negative (TN). There is no MITM attack and the classifier marked this sample as normal

(iv) False Negative (FN). There exists MITM attack and the classifier marked this sample as normal

We calculate performance measures using the following formulas based on the classification results provided above.

$$\begin{aligned}
\text{Accuracy} &= \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}, \\
\text{Precision} &= \frac{\text{TP}}{\text{TP} + \text{FP}}, \\
\text{Recall} &= \frac{\text{TP}}{\text{TP} + \text{FN}}, \\
\text{F1} &= \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}.
\end{aligned} \tag{5}$$

In the experiment, we simulated 1000 normal sessions through an automated script. The measured data is used as the initial sample, and 10 training sets are obtained from the initial sample by random sampling without putting back. The sample size of each training set is 50. The 10 training sets are used to train the classifier, respectively. We measured the RTT of 5296 IKEv1 sessions as the testing set, including 4939 normal sessions and 357 sessions attacked by man-in-the-middle. The same test set is used to test the

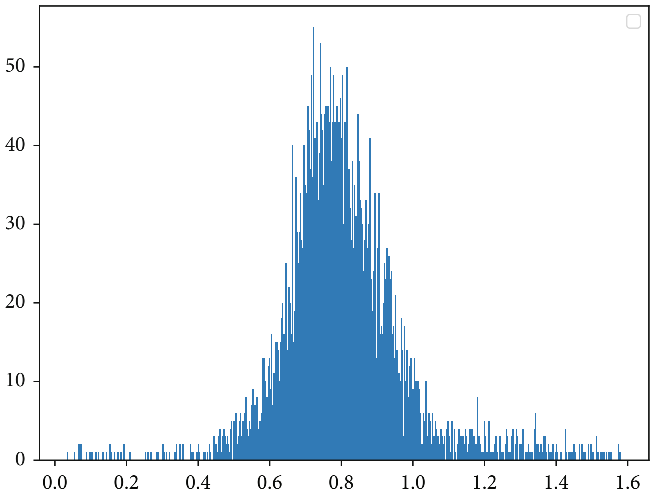

FIGURE 3: The frequency distribution histogram of RTT.

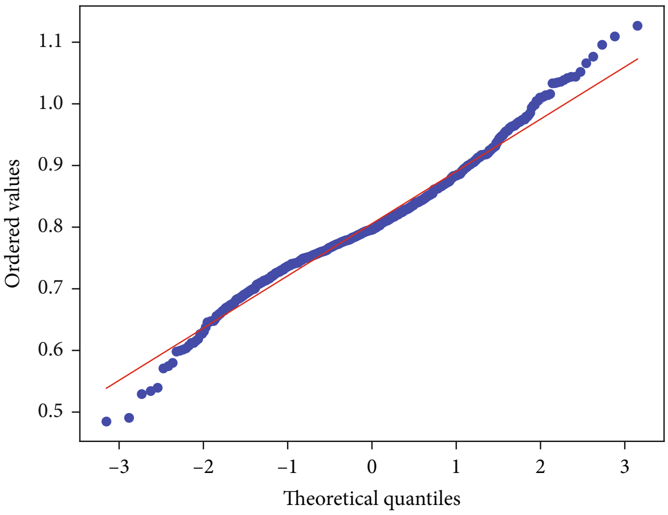

FIGURE 4: The quantile-quantile plot of RTT.

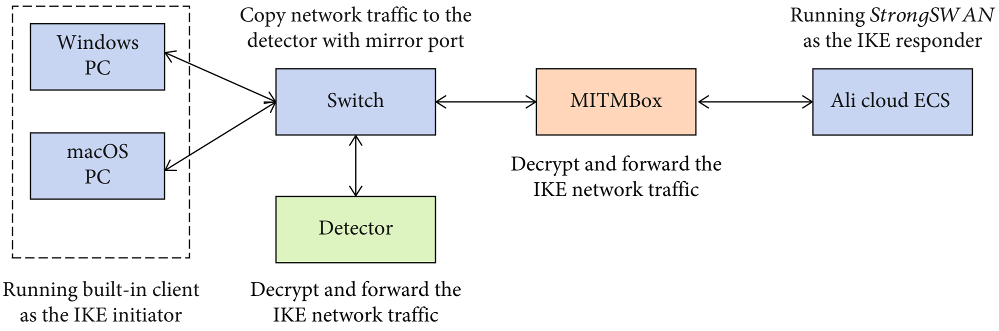
Windows PC
macOS PC
Running built-in client as the IKE initiator
Copy network traffic to the detector with mirror port
Switch
Detector
Decrypt and forward the IKE network traffic
MITMBox
Decrypt and forward the IKE network traffic
Running *StrongSWAN* as the IKE responder
Ali cloud ECS

FIGURE 5: The network topology of the Experiment.

classification performance of 10 classifiers, to evaluate the stability of the algorithm. The significance level $\alpha = 0.01$. The experimental results are shown in Table 1.

The experimental results show that the anomaly detection algorithm based on normal distribution confidence interval can identify all man-in-the-middle attacks. At the same time, some normal sessions are identified as abnormal, and the false positive rate is about 9%. The standard deviation of F1 is 0.018. It shows that the classification algorithm is stable. By comparing the experimental data, we find that the gap between normal data and abnormal data is very large. In the normal session, the mean value of ΔRTT is

Table 1: The evaluation metrics of classification.

Round	Accuracy	Recall	Precision	F1
1	0.9335	1	0.9281	0.9627
2	0.9362	1	0.9311	0.9643
3	0.9261	1	0.9202	0.9584
4	0.8095	1	0.7941	0.8852
5	0.9175	1	0.9109	0.9534
6	0.9222	1	0.9159	0.9561
7	0.9261	1	0.9202	0.9584
8	0.9373	1	0.9322	0.9649
9	0.8999	1	0.8918	0.9428
10	0.8907	1	0.8818	0.9372

1.083, while in the attacked session, the mean value of ΔRTT is 48.509; therefore, recall can reach 1.

5. Case Study

The preshared key method is easy to operate and widely used. This type of authentication method is commonly used for VPN services for sale, and it is also used by many colleges and enterprises. Because users and network administrators do not have a deep understanding of the IPSec protocol, it is generally believed that the username and password used for login are required to be kept secret, and the preshared key does not need to be kept secret. Therefore, the entropy value of the preshared key of a large number of IPSec services is too low, and some are set as the website URL and some are set as the company name; passwords such as “123456” and “VPN” are also widely used. The built-in IPSec client of common operating system platforms is imperfect from the perspective of user experience. Usually, an administrator needs to write an instruction manual for the user. The user configures the IPSec client according to the manual. The general instruction manual will indicate PSK, and many instruction manuals are completely open without any access control, which leads to the leakage of PSK. By analyzing the interaction process of the IKE protocol, an attacker can conduct a man-in-the-middle attack on IPSec communication after mastering the PSK and can decrypt the data packet and tamper with the content of the data packet, destroying the confidentiality and authentication of the protocol.

To identify the situation of PSK usage in IPSec service, we use Google to search the public PSK. For university, we use the keyword “vpn psk inurl:edu” and analyzed the top 50 results. After removing duplicate pages, inaccessible pages, and pages not related to VPN, we got 34 websites. Among these websites, there are 26 of them have public the PSK on the web pages. Within the 34 results of Google search, 76% PSK has been published on the website. In the 26 known PSK, 69% of them has less than 10 characters, 50% of the PSK contain “vpn,” 54% has some information associated with the organization, 46% of the PSK use uppercase or lowercase letters only, and 80% are in high risk of a dictionary attack.

Judging from the statistics of search results, we can infer that most network administrators do not have a thorough understanding of the IPSec protocol, which caused PSK leakage due to unconscious behavior. The PSK setting is too simple, making PSK vulnerable to dictionary attacks. The above survey reflects that there are still many security risks in the use of IPSec, which makes MITM attacks against IPSec easier to implement. In the current environment, it may be difficult to force many administrators to change their long-term behavior habits or force all IPSec users to upgrade the protocol. Therefore, it is very important to study how to detect MITM attacks against IPSec.

6. Conclusion

Since the birth of the IKE protocol, scholars have proposed a lot of improvement methods for its security. Ray et al. [9] proposed an elliptic curve cryptography (ECC) based and certificate less IKE protocol to avoid denial-of-service (DoS) attack. Yin and Wang [10] proposed an application-aware IPsec policy system on the existing IPsec/IKE infrastructure, in which a socket monitor running in the application context reports the socket activities to the application policy engine. With the application of IPsec in IoT (Internet of Things) [11–15], ICS (industrial control system) [16, 17], and other fields, its security should be paid more attention.

The related research work in this paper is a preliminary exploration of IPSec man-in-the-middle attack detection. It has been verified by experiments that during the IKE protocol interaction, the distribution of MPTTT conforms to the normal distribution, and when there is a man-in-the-middle attack during the protocol interaction, MPTTT will increase due to the addition of encryption calculations, which makes the distribution of the signal interval based on the normal distribution. Anomaly detection has become a method of IPSec man-in-the-middle attack detection. The experiments done in this paper are aimed at a specific DH-group scenario. In future research work, we will continue to study the changes in MPTTT in other scenarios. At the same time, because there is no public implementation method for IPSec man-in-the-middle attack, the research work of this paper can only be based on our own man-in-the-middle attack software. The software implementation method, hardware equipment, and optimization degree may have different effects on the experimental results. Therefore, improving the implementation method of man-in-the-middle attack equipment to make the equipment more universal is also one of our future research works.

Data Availability

The data used and/or analyzed in this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported in part by the "National Key R&D Program of China" (2021YFB2012400).

References

[1] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for virtual private networks," in *2017 International Conference on Networking, Systems and Security (NSysS)*, pp. 39–44.3, Dhaka, Bangladesh, 2017.

[2] D. Fang, P. Zeng, and W. Yang, "Attacking the IPsec standards when applied to IPv6 in confidentiality-only ESP tunnel mode," in *16th International Conference on Advanced Communication Technology*, pp. 401–405, PyeongChang, Korea, 2014.

[3] T. Mizrahi, "Time synchronization security using IPsec and MACsec," in *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pp. 38–43, Munich, Germany, 2011.

[4] K. Bhargavan and G. Leurent, "Transcript collision attacks: breaking authentication in TLS IKE and SSH," in *Network and Distributed System Security Symposium–NDSS*, pp. 1–18, San Diego, California, USA, 2016.

[5] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[6] Z. Trabelsi and K. Shuaib, "NIS04-4: man in the middle intrusion detection," in *IEEE Globecom 2006*, pp. 1–6, San Francisco, California, USA, 2006.

[7] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: using echo analysis to detect man-in-the-middle attacks in LANs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, 2019.

[8] G. Wang, Y. Sun, Q. He, G. Xin, and B. Wang, "A content auditing method of IPsec VPN," in *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) IEEE*, pp. 634–639, Guangzhou, China, 2018.

[9] S. Ray, R. Nandan, and G. P. Biswas, "ECC based IKE protocol design for internet applications," *Procedia Technology*, vol. 4, pp. 522–529, 2012.

[10] H. Yin and H. Wang, "Building an application-aware IPsec policy system," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1502–1513, 2007.

[11] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, 2668 pages, 2014.

[12] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, and U. Roedig, *Securing Internet of Things with Lightweight IPsec*, Swedish Institute of Computer Science, Kista, Sweden, 2010.

[13] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid end-to-end VPN security approach for smart IoT objectsHybrid End-to-End VPN Security Approach for Smart IoT Objects," *Journal of Network and Computer Applications*, vol. 158, article 102598, 2020.

[14] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: a surveyCurrent research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[15] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable IoT devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, article 26, pp. 1–25, 2016.

[16] T. D. Nguyen and M. A. Gondree, "Teaching industrial control system security using collaborative projects," in *Security of Industrial Control Systems and Cyber Physical Systems. CyberICS WOS-CPS 2016 2015*, A. Bécue, N. Cuppens-Boulahia, F. Cuppens, S. Katsikas, and C. Lambrinoudakis, Eds., vol. 9588 of Lecture notes in computer science, Springer, Cham, 2016.

[17] M. Nawrocki, T. C. Schmidt, and M. Wählisch, "Industrial control protocols in the Internet core: dismantling operational practices," *International Journal of Network Management*, vol. 32, no. 1, article e2158, 2022.