JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

Wireless Network Security Using WEP (Wired Equivalent Privacy) Method With RC4 Stream Cipher Encryption

Yudi Irawan Chandra[1], Nur Azis[2]

[1]Program Studi Sistem Informasi, STMIK Jakarta STI&K, Jl. BRI No.17 Radio Dalam, Kebayoran Baru, Jakarta Selatan, Indonesia 12140
[2]Program Studi Sistem Informasi, Universitas Krisnadwipayana, Jalan Raya Jatiwaringin, Pondok Gede, Kota Bekasi, Jawa Barat 13077
[1]yirawanc@gmail.com, [2]nuraziz@unkris.ac.id

Abstrak− Teknologi jaringan komputer berkembang pesat, seiring dengan meningkatnya kebutuhan akan penggunaan teknologi ini. Jaringan komputer dapat dibedakan berdasarkan ruang lingkupnya. Jaringan komputer yang mencakup area lokal dengan jarak fisik antar node yang relatif dekat, seperti di rumah, di kantor, atau universitas, dikenal sebagai Local Area Network (LAN). Jaringan Nirkabel atau Wireless LAN adalah LAN yang menggunakan gelombang radio frekuensi tinggi sebagai pengganti kabel untuk komunikasi antar nodenya. LAN nirkabel ditentukan dalam grup standar IEEE 802.11 atau lebih dikenal dengan Wi-Fi. Karena tidak menggunakan kabel, wireless LAN memungkinkan mobilitas yang tinggi bagi penggunanya. Mekanisme keamanan yang dirasa paling tepat dan memungkinkan adalah enkripsi. Dengan enkripsi, meskipun transmisi bocor dan diakses oleh orang yang tidak berhak, informasi yang terkandung di dalamnya tidak dapat diketahui tanpa kunci yang tepat. Salah satu protokol enkripsi yang digunakan dan protokol pertama pada jaringan nirkabel adalah Wired Equivalent Privacy (WEP). WEP diharapkan memberikan keamanan yang setara dengan jaringan dua kabel atau LAN kabel. Protokol ini telah ditetapkan dalam standar IEEE 802.11 (Wi-Fi), meskipun pada kenyataannya penggunaan WEP masih opsional.

Kata Kunci: Keamanan jaringan; WLAN; WEP; Enkripsi

Abstract− Computer network technology is developing rapidly, along with the increasing need for the use of this technology. Computer networks can be distinguished based on their scope. A computer network that covers a local area with relatively close physical distances between nodes, such as at home, at the office, or a university, is known as a Local Area Network (LAN). Wireless Network or Wireless LAN is a LAN that uses high-frequency radio waves as a substitute for cables for communication between its nodes. Wireless LAN is specified in the IEEE 802.11 standard group or better known as Wi-Fi. Because it does not use cables, wireless LAN allows high mobility for its users. The security mechanism that is felt to be the most appropriate and possible is encryption. With encryption, even if the transmission is leaked and accessed by unauthorized persons, the information contained in it cannot be known without the proper key. One of the encryption protocols used and the first protocol on wireless networks is Wired Equivalent Privacy (WEP). WEP is expected to provide security equivalent to a wired two network or wired LAN. This protocol has been specified in the IEEE 802.11 (Wi-Fi) standard, although in reality, the use of WEP is still optional.

Keywords: Network Security; WLANs; WEP; Encryption

1. INTRODUCTION

Wireless is a technology that aims to replace the cable that connects the computer terminal with the network. The computer can move freely and can still communicate in the network with adequate transmission speed. The IEEE standardizes wireless LAN with the code 802.II b aims to equate all wireless technologies used in the computer field and ensure interoperability between all products that use this standard.

LAN (Local Area Network) as we know it is a network that connects (interconnects) a community of Data Terminal Equipment (DTE) placed in a location (building or group). It generally uses the transmission media in the form of cables, both twisted pair and coaxial cables, also known as wired LAN. In addition, there is a LAN that was developed using the medium of radio waves or light. The advantage is that the installation cost is cheaper than wired LAN because there is no need to install too large cables, especially for sub-locations / subgroups that are a bit far away. The second consideration is that this wireless LAN is suitable for portable and mobile DTE units.

The development of wireless LAN infrastructure has also become more accessible and does not require high costs. But on the other hand, because data transmission is carried out using radio waves, security issues in wireless communication are no longer as simple as compared to wired networks. If on a wired network, physical security alone is considered sufficient (such as by restricting building access), then on a wireless network, physical restrictions are impossible to do. Radio waves used in wireless networks can penetrate building walls so that all information exchanged through these radio waves can be accessed by anyone, even by unauthorized persons. Therefore, another security mechanism needs to be implemented. One of the security methods in wireless computer networks is using the WEP method, a wireless network.security method, also known as Shared Key Authentication. Shared Key Authentication is an authentication method that requires the use of WEP. WEP encryption uses a key entered (by the administrator) to the client or access point. This key must match the one provided by the access point to the client with the one entered by the client to authenticate to the access point.

From the description that has been explained, the writer can formulate the problem as follows:

1. Explain the meaning of WEP as security on wireless LAN
2. Describe Stream Cypher RC4 as encryption on WEP

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

3. Explain the WEP configuration method on a wireless LAN computer network

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

From some of the problems that have been formulated above and because the understanding of wireless LAN network security is comprehensive, the author will limit the problem to WEP applications by using RC4 encryption as a weakness and strength of WEP. The aims and purposes of this research are:

1. Learn and understand WEP configuration on a Wireless LAN network.
2. Provides information about Stream Cypher RC4 as encryption on WEP
3. Explaining the Infrared wireless configuration in the Local Area Network.

2. RESEARCH METHODOLOGY

This writing employs a variety of strategies connected to the issue of writing in order to gather the information necessary for the creation of scientific writing, including:

a. Conduct an interview
   Interview or question and answer sessions with specialists who are knowledgeable in the subject of computer network security are recommended.
b. The act of observing
   Make firsthand observations or observations in the field or in a location that is relevant to the topic of the writing assignment.
c. Review of the Literature
   Reading books on the subject of writing or compiling documentation on the subject are two methods of approaching the problem.

3. RESULTS AND DISCUSSION

3.1 What is WEP (Wired Equivalent Privacy)

Wireless Equivalent Privacy (WEP) is an encryption algorithm that is utilized in the authentication process to verify users and encrypt data that is transmitted over the wireless network segment of a local area networking (LAN). [3][7] The IEEE 802.11 standard makes use of the WEP encryption algorithm. The WEP technique is likewise a straightforward one that makes use of a pseudo-random number generator (PRNG) and the RC4 stream cipher. For both decryption and encryption, the RC4 stream cipher is employed.

3.2. Encryption on Wireless Equivalent Privacy (WEP)

WEP employs the Stream Cipher RC4 encryption technique, which is a symmetric key encryption system that employs the same encryption key and description key for both encryption and decryption. The use of the RC4 encryption technique within the program itself is highly recommended. Furthermore, RC4 is employed in the Secure Sockets Layer (SSL) and Wi-Fi Protected Access (WPA) protocols, in addition to WEP (WPA).[4][5][6].

On the basis of the key it gets, RC4 generates a pseudorandom bit stream, also known as a Keystream, which is used for encryption (SharedKey). The keystream that has been generated is then utilized to encrypt the plaintext using the XOR technique. It is done in a similar manner to how the description process is done. Keystream is generated and XORed with the Ciphertext to create the final result.

In Wireless LANs, the IEEE 802.11 standard specifies two WEP key definition algorithms that can be utilized. All devices on a Wireless LAN system use the same shared key, which is number one. When the client obtains the appropriate key, the client is able to communicate with the system as well. The disadvantage of this approach is that it makes use of a single key, which makes it easier to compromise the security of the system.[1][2]

Two-way communications between two devices are formed using a distinct shared key for each communication session. This scheme is significantly more secure than the first method. However, as the number of devices being used grows, the distribution of key usage becomes more hard to manage.

In order to encrypt information, WEP makes use of an Initialization Vector (IV), which is a string of characters created at random and used in conjunction with a shared key. When compared to a common key, whose value is always the same, the value of IV is constantly changing. When the shared key and the new IV value are combined, the result is a key that is distinct from the prior key. It is possible that the use of IV will result in a longer Lifetime of the shared key. In most cases, the IV value used for each message sent is unique, and because IV is also provided with the message, the description process can be completed by the recipient of the message who has access to the shared key.

WEP (64-bit) is a standard security protocol that uses a 40-bit shared key and a 24-bit IV. The length of the shared key utilized in its development has varied, with 128-bit WEP employing a 104-bit shared key and 256-bit WEP employing a 232-bit shared key, among other variations. While the length of the IV used in 128-bit WEP and 256-bit WEP remained constant, precisely as long as 24-bit, the length of the IV used in 512-bit WEP increased.

Procedure The following is a diagram of the encryption process on wep:[7]

1. Initialization and generation of encryption key pairs and shared keys

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

A 40-bit shared key is used in conjunction with a 24-bit Initialization Vector that is produced at random (IV). The result is a key with a 64-bit length. This key is then used as input for the RC4 algorithm, which generates a sequence of encryption keys based on the information contained in the key.

2. Use an encryption key to protect sensitive information.
   Cylic Redundancy Check (CRC) is an algorithm that is used to ensure that data is not corrupted. When data is transferred, this method has a mechanism that prevents the data from being altered in the process. The CRC is formed as a result of the computation of the bits in the message that is to be transmitted. The result of the computation is then appended to the final portion of the message before it is sent out over the network. Receiving party can discover an error in a received message by completing computations to generate a new CRC and comparing the value of the new CRC with the value of the original CRC in the message. On the message that was sent, a 32-bit CRC procedure is done. The outcome of this procedure will be a checksum of 4 bytes in length.. After that, the checksum is appended to the end of the message. Then, using the key sequence generated by the RC4 method, this new message is XORed with the original message. This encrypted message is then sent together with the IV that has been appended to the beginning of the message, as illustrated in Figure 1.

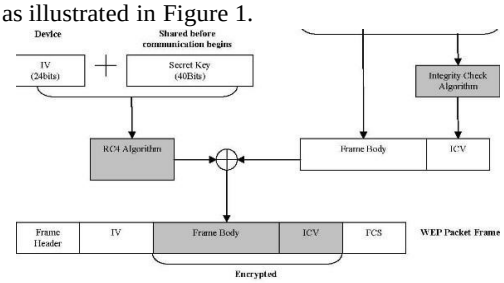

Figure 1. Encryption on WEP

3.3. RC4 Stream Cipher Encryption

An example of a stream cipher is RC4; this sort of cipher processes units of input data at a time. The data or unit of measurement is often a byte or, in some cases, a bit (byte in the case of RC4). The encryption or decryption process can be performed at a configurable length in this manner. This algorithm does not need that a specific number of input data be received before processing can begin, nor does it require that further bytes be encrypted.[9][10]

RSA Data Security, Inc. developed RC4 as a proprietary symmetric stream encryption algorithm for use in a variety of applications (RSADSI). A source code believed to be RC4 was disclosed anonymously in 1994, and the program's distribution began with that code. According to the published algorithm, the RC4 implementation on the official product is nearly identical to the published method. RC4 is a cryptographic algorithm that is widely used in a variety of applications and is generally believed to be quite safe. According to current knowledge, no one has been able to crack it; however, the 40 bit export version may be disassembled using "brute force" (trying all possible keys). RC4 is not patented by RSADSI; rather, it is not freely exchanged (trade secret).[8]

The RC4 algorithm is quite simple to comprehend. RC4 has an S-Box, S0, S1,...,S255, which has permutations ranging from 0 to 255, and permutations are functions of keys with variable length, and permutations are functions of keys with variable length. Initialization is performed on the indices I and j, which are both set to zero. The following are the procedures to take in order to produce random bytes:

i = (i + 1) mod 256
j = (j + Si) mod 256 swap Si dan Sj
t = (Si + Sj) mod 256
K = St

XORing bytes K with plaintext to produce ciphertext or XORing bytes K with ciphertext to produce plaintext is used to generate ciphertext. AES-256 encryption is extremely fast, nearly ten times as fast as DES-256 encryption. Initialization of the S-Box is similarly a simple process. To begin, enter the numbers in the sequence S0 = 0, S1 = 1,...,S255 = 255. Then fill up another 256 byte array with a key that is repeated until the full array K0, K1,...,K255 has been entirely filled with data. After setting index j to zero, perform the following steps:

for i = 0 to 255
j = (j + Si + Ki) mod 256 swap Si dan Sj

in the same permutation. To overcome this, we will use the results of the 160 bit SHA hash of our password in the implementation later on to ensure that this does not occur.

Yet another drawback is that, because RC4 encryption involves the use of an XOR operation between data bytes and the pseudo-random byte stream generated from the key, it is possible for an attacker to deduce some bits of the original message by XORing the two sets of cipher bytes, assuming that some of the input messages are

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

already known to the attacker (or easily to guess). In order to bypass this limitation, we employ an initialization vector (IV) produced using a separate ciphertext in the application. This IV does not need to be kept secret because it is simply utilized to ensure that each encryption operation generates a unique ciphertext in the first place.

The author also developed a new key initialization procedure that we refer to as SK (strengthened key), in which the user key is expanded up to 260 bytes (but only 256 bytes are used) using SHA-1 in two ways: first, the user key is used as a key; second, the first 1-20 bytes in the buffer are processed with SHA; third, the digest is placed in the first 20 bytes; fourth, bytes 1-40 are processed with SHA; and finally Afterwards, this buffer is encrypted with RC4, after which the buffer is utilized as a key once more. This last procedure is performed 16 times in order to try to mix nicely, resulting in the key being as random as possible.

There are more specifics about this procedure listed in the section below. The use of SHA in the key initialization process is not a new concept; for example, the SEAL key initialization procedure demonstrates its use of the algorithm. For key initialization, the usage of the encryption primitive process is also used in Blowfish or Cobra-128, however in a different way. According to theory, this approach would be comparable to employing a key with a total of 2048 bits, however the author himself is not certain of this (maybe some readers can provide feedback).

Despite the fact that this method appears to be a little more involved than regular key initialization, it takes less than 10ms on a Pentium 133 processor. This approach, despite the fact that the author believes it to be stronger, has not been tested, and as a result, the author provides just two options for its application: the SK way or the standard method.

Due to the fact that the encryption method is straightforward and only requires a few operations per byte, the encryption performance of RC4 is quite good. In order to put the aforesaid concept into practice, the author creates a straightforward program for file encryption. PC-Crypt version 1.0 is the name we have given to this application. This application can be built using any version of the Delphi programming language. This program has been purposefully designed to be as simple as possible, making it extremely simple to use. Depending on the application, we can utilize standard key initialization (Standard Method) or stronger key initialization (Strengthened Method) (SK Method).

Additional ASCII characters (0-255) can be entered in the key input using the "" (backslash) character, as in "PassWord25my23112245". If we enter a number that is greater than 255, it will be masked with $FF, ensuring that the result is always in the range 0-255. Meanwhile, if you want to enter the character "," you can do so by typing the letters "." The confidentiality of our password will be better preserved in this manner, as will the use of uppercase characters in the password entry.

An additional feature is the possibility to securely remove our source files. There are three solutions available for this: Delete just, Simple Method, and DoD+ Method are all options. After the encryption operation is completed, only the source file will be erased using the Delete option. In the simplest case, the source data (plaintext) will be overwritten (rewritten) once (1 pass) with a random number and then erased from the system. With regard to the DoD+ Method, the plaintext is first overwritten by the bits 11 and 00, followed by the bits 1 and 0, and finally the plaintext is overwritten by a new random number that is then deleted, as seen in the diagram below. If this option is selected during the decryption process, the ciphertext data will be removed from the system.

Those that are inventive can, of course, create their own applications, such as Cryptext, which is an extension of the Windows 95/NT shell that also employs the RC4 and SHA algorithms. We can add a compression procedure before encryption to improve data security. Because cryptanalysis relies on redundancy in the plaintext, compressing before encryption minimizes the amount of redundancy.

An additional enhancement is that when deleting source data, it is now safer to write directly to the hard drive rather than through the disk cache, because there is a risk that not all of the data has been written to the hard disk when the data is removed, as opposed to previously (because it is still in the cache). For Win32, we can accomplish this through the CreateFile API, which accepts the values FILE FLAG WRITE THROUGH and FILE FLAG NO BUFFERING, respectively.

Another approach of deletion that is more secure is the one invented by Peter Gutmann, as described in his SFS paper (so we call it the SFS method). With this SFS approach, the data is overwritten 35 times with certain bit patterns, with the goal that the magnetic surface of the hard drive will be the same as if it had been exposed to a magnetic field during the writing process. However, even in this case, he claims that advanced hardware devices can still be used to recover data (especially for old, low-density hard drives).

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

3.4. Configuration of the WEP Enabling Protocol

Because a wireless network has an open topology, it must pay greater attention to security risks than a traditional wired network would. SSID (Service Set Identifier) systems are used to ensure that only specific users can access the network at the bare minimum in wireless networks. Meanwhile, encryption technologies are employed to ensure that data transit cannot be read by third parties, hence increasing security. There are several types of authentication, including Open System, Shared Key, WPA, WPA-PKS, and 802.1X. Open System is the most widely used type of authentication.

In this module, we will solely cover the varieties of wireless access points that are available on the Linksys WRT54G WLAN AP. Authentication on the wireless AP is not enabled by default (disabled). A WLAN connection is required in order to access the access point network in this manner.

1. Configuration of the SSID

   The SSID is the initial step in being able to connect to a specific WLAN network and is used to identify the network. The default configuration of the AP is depicted in Illustration 2.

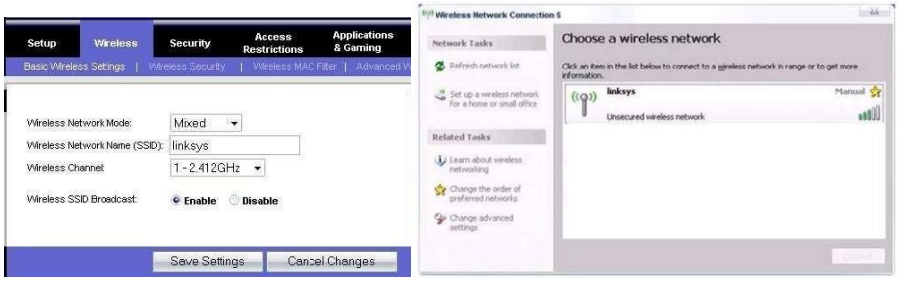

Figure 2. The default settings of the "linksys" AP and SSID are clearly accessible to the user

It is as a result of this that the "linksys" SSID is visible to the user and the "linksys" network is "unsecured," meaning that there is no authentication or encryption method in place, and therefore any user who knows the SSID is able to connect to the network. Furthermore, if the "Wireless SSID Broadcast" option is turned off, the "linksys" SSID will not be accessible to the user, and it will have to be set manually in the network configuration. The following example is carried out on a Windows computer:

a. From the "Control Panel," select "Network Connections," and you will see a list of network adapters that have been installed, including the Wireless Adapter. b. From the "Control Panel," select "Network Connections."

b. Right-click on the Wireless Adapter and select "Properties," which will bring up the wireless adapter's properties box, from which you can pick the "Wireless Networks" tab as seen in figure 3.

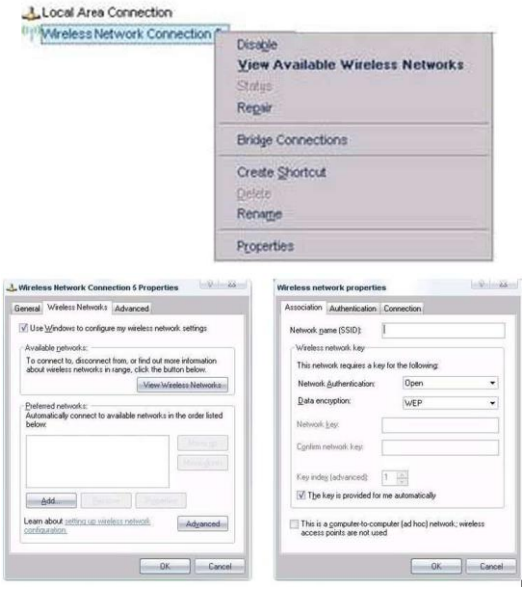

Figure 3. Windows Properties of the wireless adapter and Window Wireless Properties

WEP encryption is available in two degrees of security: 64-bit and 128-bit. The higher the encryption bit, the more secure the network; nevertheless, the network's performance drops as the encryption bit increases. Select the correct encryption bit and then enter the WEP passphrase or key in hexadecimal format to utilize WEP encryption.

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

WEP is the most often used security mode, and it is also the most secure. WEP is the use of a sequence of hexadecimal numbers produced from the encryption of a passphrase in order to establish a secure connection.

To perform the next experiment, we will enter "wawaawa" as the passphrase, then select the type of encryption bit (64 bit or 128 bit), and finally click "Generate.". Then, as seen above, four keys will be produced, each having a length of either 10 hex digits (64 bits) or 26 hex digits (128 bits). After that, decide which of the four keys will be used. Despite the fact that this is a critical parameter, it is not case sensitive. The outcomes of its implementation are depicted in the following figure 4.

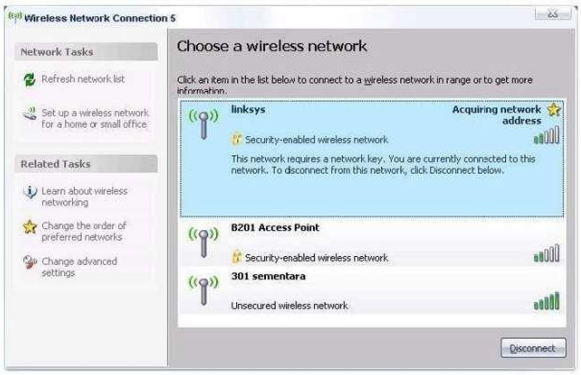

Figure 4. The results of the application of security mode

In order to establish a connection, the following Windows settings are utilized in this module:

1. Once you have opened the "Network Connections" section of the "Control Panel," you will see a list of the network adapters that have been installed, which will include the Wireless Adapter.
2. Right-click on the Wireless Adapter and select "Properties," after which the wireless adapter's properties box will display, from which you can pick the "Wireless Networks" option as seen in Figure 5 below:

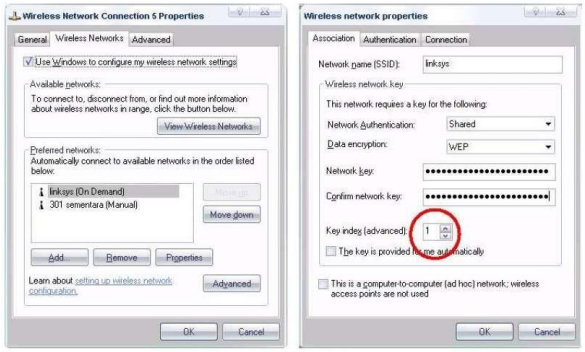

Figure 5. WEP settings

SSIDs for WLAN networks can be added to the "Preferred Networks" list by clicking "Add," but if the SSID already exists, pick it and click "Properties" until a box similar to the one shown on the top right appears, which is where we will enter our network credentials

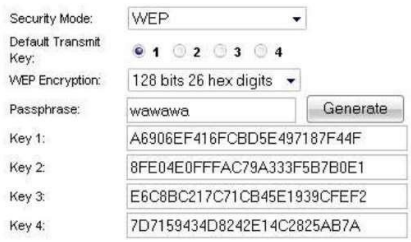

Figure 6. WEP settings on user

Figure 6 shows the selection of the SSID "linksys," the use of "Network Authentication -Shared," "Data Encryption -WEP," and "Network Key," which is filled with the corresponding Network Key according to the selected Key (between 1 and 4 choices). In this case, Key 1. is selected. Figure 7 shows the selection of the SSID "linksys," the use of "Network Authentication -Shared," "Data Encryption.

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**

JURNAL INFORMATION SYSTEM
Volume 1, Nomor 2, Bulan 2021, Page 61-67
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://journal.teknikunkris.ac.id/index.php/jis

4. CONCLUSION

The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communications (wireless) against eavesdropping and to ensure that they remain private (eavesdroppers). The WEP method is also used to prevent illegal access to a wireless network, which is the second application for it. In some cases, analyses of WEP have revealed that several aspects are not specifically targeted by the 802.11 standard, despite the fact that the standard specifies that they should be. It is expected that this will eventually become a benefit of WEP.

This section will conclude with some recommendations for improving the security of the WLAN system that can be implemented. Here are some things that need to be done if we are network administrators who are in charge of WLAN systems in a building, whether for a corporation or for our own use: Never use the default SSID; instead, customize it to your liking. If a WLAN system is still using the default SSID and password, it will be easy to assume that the system is still using the default password. Do not use the SSID to identify the company/address, division, or product name. Using names like this can draw the attention of outsiders (crackers) and entice them to investigate further into the company's WLAN network; if at all possible, avoid enabling "SSID broadcast." If SSID broadcast is enabled, the AP will receive any SSID that is broadcasted. Using this capability, you can restrict the AP's ability to accept WS to those with the right SSID and change the default password on the AP's side. Hackers and crackers can readily obtain a list of default passwords in general, as well as specific default passwords. They will attempt to utilize this default password as a starting point.

REFERENCES

[1] Nichols, Randall K., Panos Lekkas, and Panos C. Lekkas. Wireless security. McGraw-Hill Professional Publishing, 2001.
[2] Karygiannis, Tom, and Les Owens. Wireless Network Security:. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002.
[3] Wong, Stanley. "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards." SANS Institute (2003): 1-9.
[4] Borsc, M., and H. Shinde. "Wireless security & privacy." 2005 IEEE International Conference on Personal Wireless Communications, 2005. ICPWC 2005.. IEEE, 2005.
[5] Goldsmith, Andrea. Wireless communications. Cambridge university press, 2005.
[6] Security Guideline for Wireless LAN Implementation di http://www.sans.org/rr/whitepapers/wireless/ ; September 2007.
[7] Lashkari, Arash Habibi, Mir Mohammad Seyed Danesh, and Behrang Samadi. "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)." 2009 2nd IEEE international conference on computer science and information technology. IEEE, 2009.
[8] Molisch, Andreas F. Wireless communications. John Wiley & Sons, 2012.
[9] Zou, Yulong, et al. "A survey on wireless security: Technical challenges, recent advances, and future trends." Proceedings of the IEEE 104.9 (2016): 1727-1765.

Submitted: 15**/11/2021**; Accepted: 15**/11/2021**; Published: 23**/11/2021**