CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 1, Mei 2023, hlm. 1 of 5

ANALISIS PERBANDINGAN ALGORITMA *TEMPORAL KEY INTEGRITY PROTOCOL* DENGAN AES PADA ENKRIPSI WPA

Muhammad Aryanto[1], Nila Feby Puspitasari[2], Muhammad Agung Nugroho[3]

[1,2] Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
[3] Informatika, Universitas Teknologi Digital Indonesia
Email: [1] muhammad.1311@students.amikom.ac.id, [2] nilafeby@amikom.ac.id, [3] m.agung.n@utdi.ac.id

Abstrak

Pengaruh perkembangan teknologi membuat kebutuhan jaringan internet menjadi sangat penting dikarenakan dengan penggunaan internet masyarakat dapat mencari segala sesuatu informasi yang dibutuhkan. Dalam penggunaan internet pada jaringan wifi membutuhkan mekanisme keamanan jaringan. Keamanan jaringan wifi terdiri dari beberapa jenis, yaitu diantara nya adalah WEP, WPA, WPA2-PSK. Penelitian ini akan melakukan analisis perbandingan pada algoritma TKIP dan AES yang ada pada jenis keamanan WPA dengan menggunakan metode SPDLC (*Security Policy Development Life Cyle*) Didalam metode SPDLC terdiri dari identifikasi, analisis, desain, implementasi, audit, dan evaluasi. Implementasi yang dilakukan pada penelitian ini menggunakan sebuah tools *Aircrack-ng* sebagai media dalam melakukan penetrasi terhadap jenis keamanan yang akan di uji. Hasil dari penelitian ini adalah perbandingan yang dilakukan antara algoritma TKIP dan algoritma AES membuktikan bahwa algoritma AES pada WPA lebih unggul dalam mengamankan jaringan. Maka kesimpulan yang dapat diambil pada saat melakukan implementasi perbandingan algoritma TKIP dan AES pada WPA adalah kedua jenis algoritma ini masih dapat dilakukan peretasan. Hasil dari pengujian menunjukan bahwa tingkat keberhasilan dalam menemukan kata sandi memiliki tingkat keberhasilan peretasan yang tinggi yaitu dengan presentase 99,96% dan durasi selama 25 detik. Untuk jenis keamanan WPA dengan algoritma AES sedikit lebih aman meskipun masih dapat dilakukan peretasan. Dengan tingkat keberhasilan peretasan dalam menemukan kata sandi sebesar 99,30% dan dengan durasi selama 27 detik.

Kata kunci: WPA, WPA2-PSK, TKIP, AES, *Aircrack-ng*

COMPARATIVE ANALYSIS OF TEMPORAL KEY INTEGRITY PROTOCOL WITH AES

Abstract

The influence of technological developments makes the need for internet networks very important because with the use of the internet people can find all the information needed. In the use of the internet on wifi networks requires a network security mechanism. Wifi network security consists of several types, namely wep, WPA, WPA2-PSK. This research will conduct comparative analysis on existing TKIP and AES algorithms in wpa security types using the SPDLC (Security Policy Development Life Cyle) method in the SPDLC method consisting of identification, analysis, design, implementation, audit, and evaluation. The implementation carried out in this study uses a tool "Aircrack-ng" as a medium in penetrating the type of security to be tested. The result of this study is a comparison made between the TKIP algorithm and the AES algorithm proves that the AES algorithm on WPA is superior in securing the network. So the conclusion that can be taken when implementing the comparison of TKIP and AES algorithms on WPA is that these two types of algorithms can still be hacked. The results of the test show that the success rate in finding passwords has a high hacking success rate, namely with a percentage of 99.96% and a duration of 25 seconds. WPA with the AES algorithm is slightly safer for this type of security, although it can still be hacked with a hacking success rate finding passwords of 99.30% and with a duration of 27 seconds.

***Keywords**: WPA, WPA2-PSK, TKIP, AES, Aircrack-ng*

1. PENDAHULUAN

Perkembangan teknologi yang saat ini serba modern membuat kebutuhan internet sangatlah dibutuhkan oleh setiap orang, karena dengan adanya internet manusia dapat mencari segala sesuatu hal yang dibutuhkan. Supaya dapat mengakses internet diperlukan sebuah konektivitas yang dapat terhubung ke sebuah jaringan, ada banyak cara untuk dapat tersambung ke sebuah jaringan salah satu nya adalah dengan menggunakan jaringan wifi. Hampir di setiap tempat seperti mall, kantor, rumah sakit, kampus hingga rumah memiliki jaringan wifi. keamanan sistem jaringan nirkabel menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet

yang sifatnya *public* dan *global* pada dasarnya tidak aman. Adanya celah keamanan pada sistem jaringan menyebabkan kelemahan dan terbukanya celah keamanan yang dapat digunakan hacker (Yanti, 2018).

Dalam penggunaan jaringan wifi terdapat mekanisme keamanan jaringan. jenis keamanan yang terdapat di dalam jaringan wifi diantara nya yaitu. *Wired Equivalent Privacy* (WEP), *Wi-fi Protected Access* (WPA), dan *Wi-fi Protected Acces – Pre Shared Key* (WPA2 PSK). setiap jenis keamanan ini memiliki kekurangan dan kelebihan nya masing-masing seperti contoh nya keamanan yang ada pada jenis keamanan WPA. WPA ini menggunakan algoritma *Temporal Key Integrity Protocol* (TKIP) dan *Advanced Encryption Standard* (AES) sebagai media keamanannya (Qian et al., 2021).

Wireless Protected Access atau WPA adalah suatu sistem keamanan yang ada di dalam *router*. Tugas dari WPA ini adalah mengamankan jaringan nirkabel dari berbagai ancaman-ancaman yang mungkin saja terjadi. WPA ini diciptakan (Haupt, 2019) untuk melengkapi dari sistem pendahulu nya yaitu WEP. Diciptakannya WPA ini adalah dikarenakan adanya celah kelemahan pada infrastruktur nirkabel yang menggunakan jenis pengaman WEP ini. WPA mengimplementasikan layer IEEE yaitu Layer 802.11i . WPA di desain untuk menggantikan metode keamanan WEP, yang menggunakan kunci keamanan static, WPA menggunakan metode TKIP (*Temporal Key Integrity Protocol*) yang mampu berubah secara dinamis (Rahayu, 2018). Dalam melakukan konfigurasi untuk mengatur jenis keamanan WPA diperlukan alat tambahan berupa komper. Fungsi dari komputer ini kemudian dikenal dengan istilah *authentication server* yang memberikan *key* berbeda kepada masing-masing pengguna/client dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Administrator dapat memilih dari dua algoritma WPA yang di sediakan, yang terdiri dari algoritma TKIP dan AES. *National Institute of standards and technology* (NIST) mengangkat Rijndael sebagai algoritma yang disetujui sebagai *Advanced Encryption Standard* (AES). AES atau rinjdael merupakan jenis enkripsi simetris blok dimana kunci pengirim dan penerima simetris. AES memiliki tiga ukuran panjang kunci yaitu 128, 192 dan 256 bit. Blok *cipher Rjndael* di desain seluruhnya hanya menggunakan operasi byte yang sederhana. Masing masing jenis AES mempunyai variable number of rounds (Saragi, 2013).

TKIP menggunakan pemrograman WEP asli tapi "membungkus" kode tambahan pada bagian awal dan akhir untuk merangkum dan memodifikasi nya. Seperti WEP, TKIP menggunakan algoritma enkripsi *Rivest Code* 4 (RC4) *streaming chipher* yang mengenkripsi plaintext dengan menggunakan dua buah S-box yaitu *array* sepanjang 256 yang berisi permutasi dari bilangan) sampai 255 dan S-box kedia yang berisi permutasi merupakan fungsi dari kunci sebagai dasarnya.

Algoritma TKIP sendiri memiliki banyak kelemahan dibandingkan AES, sedangkan AES merupakan enkripsi yang digunakan secara umum untuk *access point* dan sudah cukup baik dari sisi keamanan untuk saat ini (Puspitasari et al., 2015). AES memiliki struktur yang lebih kuat dibandingkan dengan TKIP karena tidak menyertakan data-data sensitive seperti ketika TKIP diambil datanya oleh penyerang, satu-satunya cara untuk membobol algoritma adalah dengan metode *brute force* (Santoso et al., 2022*)*. Metode ini umum digunakan sebagai salah satu mekanisme untuk menguji keamanan pada jaringan nirkabel (Nugroho and Wibowo, 2014).

Algoritma TKIP sendiri memiliki banyak kelemahan dibandingkan AES. Sedangkan AES Enkripsi ini yang digunakan WPA/WPA2 sudah sangat kuat untuk saat ini (DAULAY, 2019). Maka dari itu peneliti ingin menguji performa dari kedua algoritma yang ada pada jenis keamanan WPA ini dan juga sebagai sarana dalam menyampaikan informasi kepada masyarakat luas terlebih kepada para pemilik maupun pemakai jaringan wifi untuk mengetahui jenis algoritma yang baik dalam mengamankan jaringan wifi. Dengan cara melakukan pengujian kepada masing-masing algoritma dengan menggunakan software *Aircrack-ng*.

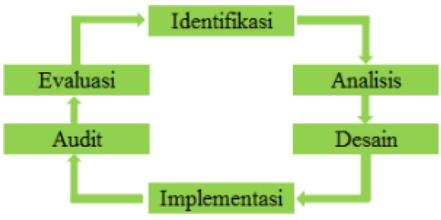
2. METODOLOGI

2.A. Metode Pengumpulan Data

Proses pengumpulan data untuk mendapatkan data yang benar dan meyakinkan, agar hasil yang dicapai tidak menyimpang dari tujuan yang telah ditetapkan sebelumnya . Pengumpulan data pada penelitian ini dilakukan dengan cara metode wawancara terhadap narasumber yang memiliki permasalahan dengan jaringan internet.

2.B. Metode Security Policy Development Life Cycle

Metode yang digunakan dalam melakukan penelitian ini adalah *Security Policy Development Life Cycle* (SPDLC) (Fitriana, 2021). Berikut merupakan tahapan-tahapan yang dilakukan dalam penelitian ini pada gambar 1.



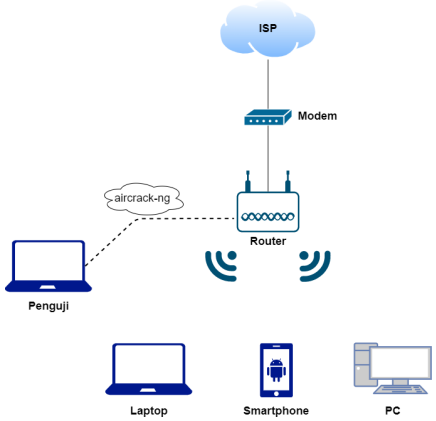
Gambar 1. Metode SPDLC

Pada proses identifikasi, hasil yang diperoleh dari pengumpulan data melalui wawancara kepada narasumber dapat diidentifikasi sebuah permasalahan yang terjadi pada jaringan wifi yaitu. dimana ketika

narasumber yang sudah berlangganan jaringan wifi selama kurang lebih satu tahun lama nya dengan menggunakan jaringan dari milik provider "Indihome" tidak memiliki permasahalan yang begitu signifikan dalam menggunakan jaringan wifi nya namun dalam beberapa minggu kebelakang barulah muncul sebuah permasalahan yang cukup mempengaruhi konektivitas jaringan nya sehingga narasumber merasakan ketidaknyamanan ketika menggunakan jaringan wifinya. Selanjutnya, pada proses analisis hasil pengumpulan data, merupakan tampilan dari serangkaian pertanyaan yang peneliti ajukan kepada narasumber. Pertanyaan yang diajukan adalah seputar jaringan wifi yang digunakan dan masalah apa saja yang terjadi selama menggunakan jaringan tersebut. Pertanyaan-pertanyaan ini nanti nya akan dilakukan Analisa terkait permasalahan yang dialami oleh narasumber.

Pada tahapan analisis permasalahan, Pengguna layanan internet nirkabel dari salah satu provider dengan brand Indihome yang sudah berlangsung selama satu tahun, tidak memiliki masalah yang begitu berarti dalam jaringan nya. Namun dalam beberapa minggu ke terakhir pengguna layanan ini mendapat permasalahan yang cukup mempengaruhi kecepatan konektivitas jaringan nirkabel miliknya tidak cepat bahkan tidak stabil. Untuk memastikan apakah ada malasah dari pusat mengenai gangguan yang terjadi ini, pengguna melakukan pengecekan melalui *call center* yang telah disedikan oleh provider tersebut. Dan diketahui permasalahan jaringan yang terjadi ini disebabkan oleh adanya perangkat lain terkoneksi ke perangkat pengguna, namun tidak diketahui/dikenal (illegal).

Pada penelitian ini tidak melakukan perancangan desain, melainkan menggunakan desain topologi yang sudah ada yaitu menggunakan topologi jaringan wifi milik dari provider Indihome. Untuk melakukan pengujian, maka dibuat skenario tertentu untuk melakukan penyerangan. Skenario ini dapat digambarkan pada gambar 2.



Gambar 2. Rancangan skenario Serangan

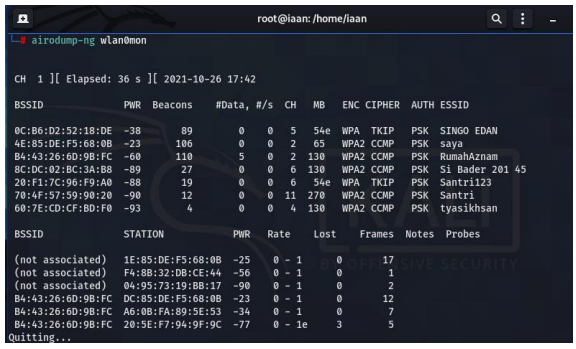
Pada gambar 2 diatas merupakan rancangan aktivitas serangan yang akan dilakukan untuk menguji pada masing-masing algoritma yang ada pada jenis keamanan WPA.

Pada proses Implementasi yang dilakukan adalah melakukan perbandingan uji performa dari kedua algoritma yaitu TKIP dan AES menggunakan tools *Aircrack-ng* agar mendapatkan bukti nyata berupa visual dari masing-masing algoritma yang di uji. Proses selanjutnya, audit dilakukan bertujuan untuk memastikan bahwa penelitian sudah dilakukan sejalan dengan perancangan yang sudah ditentukan sebelum dilakukannya implementasi demi mendapatkan hasil yang diinginkan.

Setelah menjalankan proses implementasi yang menguji algoritma TKIP dan algoritma AES pada WPA dilakukan evaluasi terkait variable yang di uji supaya hasil yang di dapat benar-benar telah sesuai dengan tujuan dilakukan nya penelitian ini. sebelum hasil tersebut sampai kepada masyarakat luas yang membutuhkan informasi mengenai keamanan jaringan wifi.

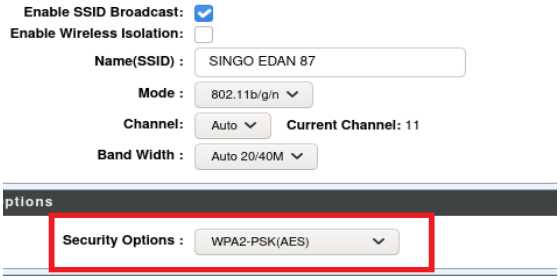
3. PEMBAHASAN

Proses pengujian diawali dengan melakukan scanning jaringan wifi tujuan nya adalah agar mengetahui BSSID, PWR, dan ESSID pada jaringan wifi yang akan di uji. Jaringan yang akan di uji adalah wifi dengan ESSID "SINGO EDAN" yang menggunakan jenis algoritma AES Seperti pada Gambar 3.



Gambar 3. *Scanning* wifi

Pada penelitian dilakukan konfigurasi dari sisi *wireless access point* beserta konfigurasi algoritma TKIP dan AES yang digunakan. Secara teknis, model konfigurasi pada *wireless client* menggunakan authentikasi WPA dan algoritma TKIP dan AES. Proses konfigurasi pada perangkat wireless access point digambarkan pada gambar 4.



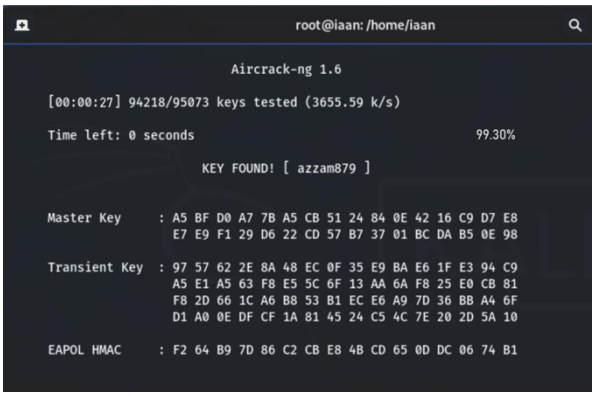
Gambar 4. Mekanisme konfigurasi untuk pengujian

Proses pengujian dilakukan terhadap model konfigurasi dari algoritma TKIP pada WPA. Setelah dilakukan pengujian terhadap jenis keamanan WPA dengan algoritma TKIP diperoleh hasil dengan tingkat keberhasilan 99,96% dengan waktu yang dibutuhkan rata-rata adalah 25 detik. Hasil dari pengujian ini dapat dilihat pada gambar 4. Proses pengujian ini menggunakan aircrack-ng versi 1.6 dengan menggunakan kemungkinan jumlah kunci yang diujicoba atau *keys tested* sejumlah 95073 kunci. Pada proses pengujian ini diperoleh kata kunci atau *password* dari WPA dengan algoritma TKIP yaitu azzam879.

Gambar 4. Hasil pengujian keamanan WPA dengan TKIP

Pada tahapan selanjutnya, dilakukan pengujian dengan model authentikasi WPA namun menggunakan algoritma AES. Pada proses pengujian seperti pada gambar 5, diperoleh hasil dengan tingkat keberhasilan adalah 99,30% dengan waktu proses *cracking* adalah 27 detik. Proses pengujian ini menggunakan *aircrack-ng* versi 1.6 dengan menggunakan kemungkinan jumlah kunci yang diujicoba atau *keys tested* sejumlah 95073 kunci. Pada proses pengujian ini diperoleh kata kunci atau password dari WPA dengan algoritma AES yaitu azzam879. Dari kedua perbandingan tersebut dapat menggunakan *data gathering* yang sama pada saat melakukan proses *sniffing* pada perangkat *wireless access point*. Jika kedua data pengujian *cracking* diperbandingkan, maka dibutuhkan waktu yang lebih lama untuk melakukan proses *cracking* pada algoritma AES dengan data *sniffing* yang sama.

Namun baik menggunakan algoritma TKIP ataupun AES tingkat keberhasilan dari proses *cracking* tergolong tinggi yaitu diatas 99%. Secara keseluruhan, hasil yang telah didapatkan dari 20 kali pengujian kepada masing-masing algoritma dengan menggunakan tools *aircrack* dan juga *wordlist* sebagai tebakan kata sandi nya yang berjumlah 95073 kata. Setelah dilakukan pengujian kepada masing masing algoritma yang ada pada jenis keamanan WPA. berikut merupakan hasil yang didapatkan dari pengujian masing-masing algoritma yaitu durasi waktu yang dibutuhkan untuk mendapatkan kata sandi dengan algoritma AES lebih unggul daripada algoritma TKIP; Presentase keberhasilan peretasan tertinggi yang diperoleh TKIP yaitu 99.96% pada pengujian ke 20; Presentase keberhasilan peretasan tertinggi yang di peroleh AES yaitu 99.30% pada pengujian ke 4.



Gambar 5. Hasil pengujian WPA dengan algoritma AES

4. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dijelaskan dan dibuktikan di atas telah didapatkan hasil dari perbandingan antara algoritma TKIP dan AES pada jenis keamanan WPA, maka dapat disimpulkan bahwa jenis keamanan WPA dengan algoritma TKIP dan AES masih dapat ditembus keamanan nya oleh aplikasi *aircrack-ng* meskipun algoritma AES ini sudah merupakan yang terbaik untuk saat ini. Keamanan WPA dengan algoritma TKIP cenderung tidak aman, karena ketika dilakukan pengujian perbandingan dengan algoritma AES. Hasil dari pengujian menunjukan bahwa tingkat keberhasilan dalam menemukan kata sandi memiliki tingkat keberhasilan peretasan yang tinggi yaitu dengan presentase 99,96% dan durasi selama 25 detik. Untuk jenis keamanan WPA dengan algoritma AES sedikit lebih aman meskipun masih dapat dilakukan peretasan. Dengan tingkat keberhasilan peretasan dalam menemukan kata sandi sebesar 99,30% dan dengan durasi selama 27 detik.

DAFTAR PUSTAKA

DAULAY, M.I., 2019. Analisis Perbandingan Keamanan WEP, WPA, WPA2, Pada Access Point (PhD Thesis). Universitas Islam Riau.

FITRIANA, Y.B., 2021. Analisis Network Security Komputer Tingkat Desa Menggunakan

Metode Security Policy Development Life Cycle (SPDLC). J. Tek. Juara Aktif Glob. Optimis 1, 11–21.

HAUPT, R.L., 2019. Wireless Communications Systems: An Introduction. John Wiley & Sons.

NUGROHO, M.A., Wibowo, F.W., 2014. Mapping of quality of service parameter with monitoring end-to-end method of ITU-T Y. 1541 standard in the hotspot area. Adv. Sci. Lett. 20, 259–263.

PUSPITASARI, N.F., Al Fatta, H., Wibowo, F.W., 2015. Implementation of greedy and simulated annealing algorithms for wireless access point placement, in: 2015 3rd International Conference on Artificial Intelligence, Modelling and Simulation (AIMS). IEEE, pp. 165–170.

QIAN, Y., YE, F., CHEN, H.-H., 2021. Security in Wireless Communication Networks. John Wiley & Sons.

RAHAYU, S.R., 2018. Laporan Tugas Komdat Tracking SSID menggunakan Wigle Wifi [WWW Document]. Track. SSID Menggunakan Wigle Wifi.

SANTOSO, N.A., AINUROHMAN, M., KURNIAWAN, R.D., 2022. PENERAPAN METODE PENETRASION TESTING PADA KEAMANAN JARINGAN NIRKABEL. J. Responsif Ris. Sains Dan Inform. 4, 162–167.

SARAGI, J.A.P., 2013. IMPLEMENTASI SISTEM KEAMANAN JARINGAN WIRELESS YANG MENERAPKAN WEP, WPA, DAN WPA2. Universitas Telkom.

YANTI, Y., 2018. Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi. J. Serambi Eng. 3.