RANCANG BANGUN SISTEM KEAMANAN ANTI *EVIL TWIN* (ANET) BERBASIS RASPBERRY PI

Muhammad Iqbal Nugraha[1] , Asri Wulandari[2]
Politeknik Negeri Jakarta, Jurusan Teknik Elektro, Prodi Broadband Multimedia,
Jl prof.Dr.GA Siwabessy, Kampus Baru UI Depok 16425
e-mail: muhammad.iqbalnugraha.te17@mhsw.pnj.ac.id

ABSTRACT

Wei defines Evil Twin as an attack which makes the user connect to a Rogue Access point because the Rogue Access Point mimics a legitimate Access point (AP), and then the attacker will take advantage of that. Anti Evil Twin (ANET) is a Program planted in Raspberry Pi, which is useful for detecting the Evil Twin and attack the Evil Twin. ANET can detect Evil Twin by creating a whitelist of legitimate Access Point BSSID and SSID. Then Anet will monitor the Air Interface to see if there is any AP with the same SSID as in the Whitelist but the BSSID is different from the one in the Whitelist. If ANET finds an AP with exact criteria, then it is the Evil Twin. ANET can eradicate Evil Twin by sending a deauthentication attack which will flood the Evil Twin traffic data, and then no user wants to connect to Evil Twin. ANET accuracy result in detecting Evil Twin is 100% with 105 tests. And the test for ANET to eradicate the Evil Twin is successful in comparison before and after the deployment of ANET.

Key words: Deauthentication; Evil Twin; Raspberry Pi; Whitelist Access Point

ABSTRAK

Wei mendefinisikan serangan Evil Twin sebagai serangan yang membuat pengguna Wi-Fi terjebak untuk terhubung kepada Access Point palsu yang dibuat mirip dengan Access Point asli, dan ketika ada pengguna Wi-Fi yang terjebak maka akan dimanfaatkan oleh penyerang untuk tujuan tertentu. Program yang dibuat merupakan aplikasi yang berfungsi untuk mendeteksi keberadaan Evil Twin serta melakukan tindakan kepada Evil Twin tersebut dan ditunjukan dalam Raspberry Pi. Aplikasi ini dinamakan ANET (Anti Evil Twin), Cara kerja dari ANET dalam mendeteksi keberadaan Evil Twin adalah dengan membuat daftar whitelist dari BSSID dan SSID Access Point yang ingin dilindungi, lalu ANET akan melakukan monitoring terhadap Air interface untuk melihat apakah ada Access Point yang SSID nya mirip dengan Access Point yang ingin dilindungi, namun BSSID nya di luar dari whitelist yang sudah dibuat. Ketika ada Access Point yang memenuhi ketentuan tersebut, maka itulah Evil Twin nya. Cara kerja ANET dalam membasmi keberadaan Evil Twin adalah dengan cara mengirimkan paket paket deauthentication kepada Evil Twin, sehingga trafik data dari Access Point Evil Twin hanya penuh dengan paket paket deauthentication, sehingga tidak ada lagi pengguna yang akan terhubung kepada Evil Twin. Hasil dari pengujian ANET dalam mendeteksi keberadaan Evil Twin mencapai 97% dengan 105 kali percobaan, sedangkan pengujian ANET dalam membasmi keberadaan Evil Twin mencapai tingkat berhasil dengan perbandingan antara sebelum adanya perlindungan ANET dan setelah adanya perlindungan ANET.

Kata Kunci: Deauthentication; Evil Twin; Raspberry Pi; Whitelist Access Point

PENDAHULUAN

Dimasa Industri 4.0 seperti sekarang ini, internet merupakan tulang punggung bagi kelancaran berkomunikasi dan bertukar informasi. Beragam teknologi mulai diluncurkan sebagai solusi agar komunikasi berbasis internet menjadi lebih fleksibel dan mudah, seperti jaringan seluler, fiber optik sampai Wi-Fi. Wi-Fi menawarkan kemudahan dalam mobilitas penggunanya sehingga membuat banyak orang tertarik untuk memanfaatkannya, terhitung selama tahun 2019 ada 3.05 miliar *Access Point* (AP) Wi-Fi yang aktif di seluruh dunia [1] dan akan terus bertambah seiring dengan naiknya kebutuhan masyarakat akan internet di masa mendatang.

Namun kemudahan mobilitas yang ditawarkan oleh Wi-Fi juga berpasangan dengan kelemahannya, yaitu kerentanan dari sisi keamanan. Hal ini terjadi karena Wi-Fi menggunakan udara sebagai media komunikasi antar perangkat penggunanya, dan lalu lintas paket-paket data yang tersebar di udara bisa diamati oleh siapa saja yang memiliki perangkat yang sesuai. Ini menyebabkan mudahnya informasi pengguna di sadap oleh penjahat yang hanya perlu berada di dalam radius sinyal Access Point (AP) dan menjalankan perangkat penyadap nya seperti laptop, *smartphone* dan perangkat lainnya. Selain menyadap, serangan terhadap kerentanan yang terdapat dalam Wi-Fi juga beragam seperti *Man-In-The-Middle* (MITM) *Attack*, *deauthentication flood*, *mac spoofing*, *Rogue Access Point* dan lainnya [2]

Salah satu serangan yang paling sering terjadi kepada Wi-Fi adalah *Rogue Access Point*, yaitu *Access Point* palsu yang tidak dipasang oleh admin resmi suatu jaringan [3]. Mengingat pentingnya keamanan Wi-Fi di dalam era komunikasi digital seperti sekarang ini, maka penulis akan membuat aplikasi yang bisa mendeteksi *Evil Twin* dengan metode algoritma "*Whitelist Access Point"* dan juga menindak *Evil Twin* yang sudah terdeteksi. Aplikasi ini akan dinamakan sebagai "ANET" (*Anti Evil Twin*)

Tujuan dari penulisan ini adalah untuk membuat alat yang bisa mendeteksi keberadaan dari *Evil Twin* secara tepat serta melakukan tindakan terhadap *Evil Twin* yang terdeteksi.

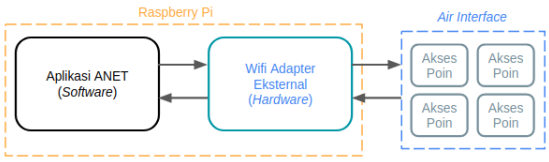
METODE PENELITIAN

Rancang bangun perangkat ini meliputi tahap perancangan, realisasi, dan pengujian.

Spesifikasi aplikasi yang dirancang untuk sistem peminjaman proyektor memiliki kemampuan untuk:

1. Mendeteksi keberadaan sebuah *Evil Twin*
2. Melakukan serangan *Deauthentication flood* kepada *Evil Twin* yang terdeteksi
3. Merekam aktifitas yang terjadi selama proses mendeteksi dan menyerang *Evil Twin* berlangsung.

Rancangan terdiri dari memprogram algoritma pendeteksi dan pembasmi *Evil Twin*, merancang *layout* dari aplikasi, dan mengintegrasikan antara algoritma dengan *layout* yang sudah dibuat. Dibawah ini merupakan diagram blok dari program aplikasi ANET.



Gambar 1. Diagram Blok Sistem

Pada Gambar 1, terlihat bahwa aplikasi ANET masih berada di dalam Raspberry Pi, ANET terhubung dengan Wi-Fi *Adapter* Eksternal untuk melakukan pemantauan terhadap *Air Interface*, pemantauan ini dilakukan sebagai langkah inti dari melakukan pendeteksian *Evil Twin*. Lalu bilamana ada *Evil Twin* yang terdeteksi, maka ANET akan langsung mengirim perintah kepada Wi-Fi *Adapter* agar

langsung membanjiri *Evil Twin* dengan paket-paket *deauthentication*.

ANET disusun atas komponen *hardware* dan juga *software*. Rincian mengenai spesifikasi dari komponen yang dipakai akan dituangkan dalam Tabel 1 dan Tabel 2 sebagai berikut.

Table 1. Spesifikasi Komponen *Hardware*

No	Nama *Hardware*	Spesifikasi
1	Raspberry Pi 4B	RAM 4 GiB; CPU ARMv8 64 bit @1.4 GHz
2	Sandisk Ultra External SD Card	Kapasitas 32 GB; Kecepatan baca 100 MBps
3	Wi-Fi *Adapter* Eksternal TP Link WN722N	*Wireless Standard* 802.11 b/g/n; Frekuensi 2.4 GHz; Chipset Atheros AR9271; 4 dBi *Gain Antenna*

Pada Tabel 1 terlihat bahwa koponen *hardware* yang ANET gunakan bias dibagi menjadi 2 bagian utama, yaitu bagian "otak" yaitu yang memproses algoritma, diwakili oleh Raspberry Pi dan SD Card, sedangkan bagian "tangan" yaitu bagian yang melakukan kegiatan di *air interface*, diwakili oleh Wi-Fi Adapter Eksternal, Adapun Spesifikasi komponen *software* yang digunakan ANET akan dicantumkan pada Tabel 2 sebagai berikut.

Tabel 2. Spesifikasi Komponen *Software*

No	Nama *Software*	Spesifikasi
1	Raspberry Pi OS	Rilis 4 Maret 2021; Versi Kernel 5.10; Arsitektur 32 bit
2	Python	Versi 3.8.5
3	Aircrack-ng suite	Versi 1.6.0
4	tmux	Versi 3.0A
5	Geany	Versi 1.36 "Poliff"

Pada Tabel 2 diterangkan bahwa komponen *software* yang dipakai untuk menyusun ANET itu mayoritasnya merupakan *software* untuk menyusun kinerja ANET yang berfokus kepada kegiatan mendeteksi serta membasmi keberadaan *Evil Twin.*

Software Aircrack-ng memang sudah sering digunakan dalam kegiatan untuk melakukan analisis trafik *Air Interface*. Bahkan *Software* tersebut sering digunakan untuk mengaudit keamanan suatu perangkat nirkabel untuk diketahui apakah tingkat keamanan dari perangkat tersebut sudah terjamin ataukan masih harus ada perbaikan lagi.

Adapun *flowchart* perancangan sistem ANET ditampilkan pada Gambar 2.

Gambar 2. *Flowchart* perancangan ANET

Tahap - tahap dalam merancang sistem ANET yang dilakukan adalah:

1. Merancang Algoritma untuk mendeteksi keberadaan dari *Evil Twin*, Algoritma yang dipakai akan berdasar kepada metode *Whitelist Access Point.* Algoritma akan ditulis dalam Bahasa pemrograman "Python".
2. Melakukan perancangan layout untuk memberikan kemudahan pengguna dalam mengoprasikan aplikasi ANET.
3. Melakukan Integrasi antara Algoritma yang sudah dibuat dengan *layout* yang sudah dirancang, dan inilah tahap akhir dari penyusunan aplikasi ANET.

Agar aplikasi ANET bisa berfungsi sebagaimana tujuan awal, maka ANET perlu diuji dengan beberapa pengujian. Langkah – langkah pengujian yang dilakukan adalah sebagai berikut:

1. Pengujian Tingkat akurasi ANET dalam mendeteksi keberadaan 1 buah *EvilTwin*.
   Adapun tingkat akurasi ANET bisa diukur sebagai berikut (%) =
   $$\frac{c}{t} x\ 100\% \quad (1)$$
   c = Jumlah deteksi *Evil Twin* yang tepat
   t = Total pengujian pendeteksian yang dilakukan
   ANET bisa dikatakan berhasil apabila memiliki tingkat akurasi mencapai 96,1 % [4].

2. Pengujian ANET dalam mendeteksi keberadaan 2 buah *Evil Twin*.

   Pengujian ini dilakukan sebagai pembanding dari pengujian 1. Yang membedakan adalah jumlah *Evil Twin* yang dipasang.

3. Pengujian ANET dalam membasmi *Evil Twin.*

   Pengujian ini dilakukan untuk melihat apakah ANET dapat memberikan dampak dalam mencegah pengguna Wi-Fi agar tidak terjebak kedalam *Evil Twin*.

Hasil dan Pembahasan

Ketika selesai melakukan pengujian, akan dilihat hasil dari masing masing pengujian tersebut untuk kemudian di analisis hasilnya. Berikut hasil dari masing masing pengujian tersebut.

1. Hasil Pengujian Tingkat Akurasi ANET dalam mendeteksi keberadaan 1 buah *Evil Twin*.

Dalam melakukan pengujian Tingkat akurasi ANET dalam mendeteksi keberadaan *Evil Twin*, maka didapat data pengujian seperti yang tertuang dalam Tabel 3.

Tabel 3. Hasil Pengujian Pnedeteksian 1 buah *Evil Twin*

Bagian	Percobaan dilakukan	Jumlah deteksi tepat	Jumlah deteksi meleset
1	35	33	2
2	35	35	0
3	35	34	1
Total	105	102	3

Dalam Tabel 3 dijelaskan bahwa ANET bisa mendeteksi keberadaan *Evil Twin* secara tepat sebanyak 102 kali dari total 105 kali pnedeteksian. Sehingga ketika angka akurasi tersebut dimasukan kedala rumus ke (1) , maka akan diperoleh nilai tingkat akurasi sebagai berikut.

$$\frac{102}{105} x\ 100\% = 97.14\%$$

Batas minimal tingkat akurasi yang ditetapkan untuk algoritma *whitelist Access Point* adalah sebesar 96%[4]. Maka dalam pengujian ini, ANET bias dikatakan berhasil dalam melakukan pendeteksian 1 buah *Evil Twin.*

2. Hasil Pengujian ANET dalam mendeteksi keberadaan 2 buah *Evil Twin*.

Dalam pengujian ANET mendeteksi keberadaan 2 buah *Evil Twin* secara sekaligus, maka didapat hasil pengujian seperti yang tertuang dalam Tabel 4.

Tabel 4. Hasil Pengujian Pnedeteksian 2 buah *Evil Twin*

	Evil Twin 1	*Evil Twin* 2
Percobaan 1	1	0
Percobaan 2	1	0
Percobaan 3	0	1
Percobaan 4	0	1
Percobaan 5	0	1
Percobaan 6	0	1
Percobaan 7	1	0
Percobaan 8	1	0
Percobaan 9	1	0
Percobaan 10	0	1
Total	5	5

Dalam Tabel 4 dijelaskan bahwa ANET hanya mampu mendeteksi keberadaan 1 buah *Evil Twin* saja selama waktu tertentu, hal ini disebabkan karena algoritma ANET yang dipasang dengan ketentuan apabila ada sebuah *Evil Twin* terlihat, maka langsung dilakukan penyerangan terhadap *Evil Twin* tersebut.

Sehingga ANET tidak akan sempat dalam melakukan deteksi keberadaa *Evil Twin* lainya ketika sedang dalam proses penyerangan terhadap suatu *Evil Twin*.

Dalam pengujian ini, ANET diputuskan gagal dalam melakukan pendeteksian terhadap lebih dari 1 buah *Evil Twin* secara bersamaan.

3. Pengujian ANET dalam membasmi *Evil Twin.*

Dalam pengujian ANET membasmi keberadaan *Evil Twin*, maka akan dibuat menjadi 2 buah scenario, scenario 1 menunjukan ketika ada *Evil Twin* namun AENT tidak melakukan tindakan apapun terhadap *Evil Twin*, dan scenario 2 menunjukan ketika ada *Evil Twin* yang kemudian secara langsung ditindak oleh ANET. Untuk hasil dari scenario 1 maka akan ditampilkan dalam Tabel 5.

Tabel 5. Hasil Pengujian Skenario 1

	Skenario 1	
	AP dan C	ET dan C
Paket terkirim (*upstream)*	101	621
Paket diterima (*downstream)*	188	803
Deauthentication	0	0

Dalam Tabel 5 Dijelaskan bahwa ketika ada *Evil Twin* muncul, maka ANET akan diam saja, maka efek dari kejadian ini adalah Client akan lebih cenderung untuk terhubung kepada *Evil Twin*, bias terlihat dari total paket yang terjadi antara Clinet dan Evil Twin itu lebih banyak daripada antara Client dengan Access point.

Untuk hasil pengujian scenario ke 2, maka akan dimuat dalam Tabel 6 sbeagai berikut.

Tabel 6. Hasil Pengujian Skenario 2

	Skenario 2	
	AP dan C	ET dan C
Paket terkirim (*upstream)*	85	7
Paket diterima (*downstream)*	217	8
Deauthentication	0	14239

Pada Tabel 6, dapat dilihat bahwa hubungan antara Client dengan Access Point itu lebih banyak dibandingkan hubungan antara Client dengan Evil Twin. Hal ini terjadi karena ketika Evil Twin muncul, maka ANET akan langsung menyerang Evil Twin tersebut dengan paket paket *deauthentication*, yng menyebabkan hubungan komunikasi antara *client* dan Evil Twin menjadi terganggu.

Ketika Evil Twin diserang, maka Client akan mencari Access Point lain yang lebih bias diandalkan, maka pilihan akan jatuh ke Access point asli, hal inilah yang membuat hubungan antara Client dan Access Point menjadi lekat kembali.

Dalam pengujian ini, ketika membandingkan antara scenario 1 dan scenario 2, dapat ditarik kesimpulan bahwa ANET berhasil memberikan dampak dalam mencegah Client agar tidak terjebak kedalam Access Point palsu (Evil Twin).

KESIMPULAN

1. ANET dibuat untuk mendeteksi keberadaan Evil Twin serta dirancang untuk langsung menindak Evil Twin yang terdeteksi.
2. Berdasarkan pengujian tingkat akurasi ANET dalam mendeteksi keberadaan 1 buah Evil Twin, nilai akurasi bernilai 97.4% dalam pengujian terhadap 3 Access Point berbeda dengan total pengujian mencapai 105 kali.
3. Berdasarkan pengujian tingkat akurasi ANET dalam mendeteksi keberadaan 2 buah Evil Twin, disimpulkan bahwa ANET gagal dalam mendeteksi lebih dari 1 buah Evil Twin secara bersamaan.
4. Berdasarkan pengujian ANET dalam membasmi Evil Twin, ANET berhasil memberikan dampak agar pengguna tidak terhubung kepada Evil Twin.

DAFTAR PUSTAKA

[1] Research and Market (2020). Global Wi-Fi Enabled Devices Shipment Forecast, 2020-2024

[2] Agarwal, M., Biswas, S., & Nandi, S. (2018). An Efficient Scheme to Detect *Evil Twin* Rogue Access Point Attack in 802.11 Wi-Fi Networks. *International Journal of Wireless Information Networks, 25*(2), 130-145. doi:10.1007/s10776-018-0396-1

[3] Alotaibi, B., & Elleithy, K. (2016). Rogue Access Point Detection: Taxonomy, Challenges, and Future Directions. *Wireless Personal Communications, 90*(3), 1261-1290. doi:10.1007/s11277-016-3390-x

[4] Kao, K., Yeo, T., Yong, W., & Chen, H. (2011). A location-aware rogue AP detection system based on wireless packet sniffing of sensor APs. *Proceedings of the 2011 ACM Symposium on Applied Computing - SAC '11*. doi:10.1145/1982185.1982195