Analisis, Serangan, dan Pendeteksian Serangan pada Protokol Kriptografi *Wi-Fi Protected Setup* (WPS)

Michael Alexander Wangsa
Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
michaelaw320@gmail.com

***Abstract*—Paper ini membahas protokol kriptografi WPS, serangan yang dapat dilakukan, analisis terhadap serangan yang dapat dilakukan, serta usulan pendeteksian serangan terhadap protokol WPS sebagai *man-in-the-middle*.**

Keywords—Protokol kriptografi; WPS; Wi-Fi; brute force; serangan; pendeteksian serangan.

I. PENDAHULUAN

Jaringan nirkabel (*Wireless Network*) berkembang sebagai alternative dari jaringan kabel yang bertujuan memudahkan penghubungan perangkat ke dalam sebuah jaringan. Saat ini, sudah banyak perangkat yang mendukung atau hanya menyediakan akses ke jaringan melalui jaringan nirkabel. Jaringan nirkabel pada awalnya tidak memiliki keamanan sehingga dikembangkanlah beberapa standar untuk mendukung keamanan informasi yang ditransmisikan melalui jaringan radio nirkabel di antaranya adalah WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*), dan yang terbaru adalah WPA2 (*Wi-Fi Protected Access II*). Saat ini sebagian besar jaringan menggunakan standar WPA2 sebagai pengamanannya karena pengamanan standar terdahulu (WEP dan WPA) sudah tidak aman lagi.

Standar WPA2 mensyaratkan perangkat yang ingin tergabung ke dalam jaringan nirkabel mengetahui sandi dari jaringan tersebut. Pada tahun 2006, *Wi-Fi Alliances*, sebuah badan yang mengatur standar dari jaringan nirkabel, mengeluarkan sebuah protokol kriptografi yang bermaksud memudahkan pengguna untuk masuk ke dalam jaringan nirkabel yang diamankan oleh standar WPA2 dinamakan WPS (*Wi-Fi Protected Setup*) atau *Wi-Fi Simple Configuration* (WSC). Namun, pada tahun 2011, celah keamanan ditemukan pada protokol kriptografi WPS. Dengan perkakas dan teknik yang tepat, seseorang dapat mengetahui sandi dari jaringan yang diamankan oleh WPA2 dengan memanfaatkan celah keamanan dari protokol kriptografi WPS [1].

Makalah ini akan berfokus kepada penjelasan tentang cara kerja protokol kriptografi WPS khususnya mode PIN *External Registrar*, peran kriptografi dalam pengamanan pesan yang dipertukarkan oleh protokol WPS, serangan yang dapat dilakukan terhadap protokol WPS, serta usulan solusi dalam melakukan pendeteksian dari percobaan serangan terhadap protokol WPS khususnya pada metode PIN.

II. *WI-FI PROTECTED SETUP* (WPS)

Wi-Fi Protected Setup (WPS) adalah sebuah protocol berbasiskan kriptografi yang digunakan untuk mengirimkan konfigurasi atau melakukan konfigurasi sebuah perangkat jaringan nirkabel melalui medium yang tidak aman. Ada beberapa moda atau metode dalam protokol WPS di antaranya adalah *Push Button* (PBC), *Personal Identification Number* (PIN), *Near-field Communication* (NFC), dan USB. Metode PBC, NFC, dan USB dianggap aman karena untuk menginisiasi mode WPS dibutuhkan akses fisik terhadap *Access Point* (AP).

Protokol WPS mendefinisikan tiga tipe perangkat dalam sebuah jaringan [2].

1. *Enrolee*, perangkat yang tidak mempunyai konfigurasi untuk jaringan nirkabel.
2. *Registrar*, perangkat yang mempunyai konfigurasi jaringan nirkabel.
3. *Access Point*, perangkat yang menyediakan jaringan nirkabel dan meneruskan pesan antara *enrolee* dan *registrar*.

Pada metode PIN ada dua cara untuk bergabung ke jaringan nirkabel. Pertama adalah *Internal Registrar*, dimana pengguna memasukkan PIN dari *wireless adapter (enrolee)* ke dalam *Web Interface* atau perangkat masukan lainnya dari *Access Point* yang merangkap sebagai *registrar*. Pada cara ini, *enrolee* akan mendapatkan konfigurasi jaringan *access point* setelah memasukkan PIN *enrolee* dengan benar ke dalam *interface* dari *registrar*.

Cara kedua disebut *External Registrar* ketika PIN dari *access point* dimasukkan pada perangkat *client* [1] [3]. Cara ini digunakan saat melakukan konfigurasi awal atau konfigurasi ulang dari perangkat *access point.* Pada cara ini, *access point* dianggap sebagai *enrolee* yang akan dikonfigurasi dan pemilik

konfigurasi adalah *client* (*registrar*). Jika keadaan *access point* sudah terkonfigurasi, sebelum konfigurasi ulang dilakukan oleh *client* kepada *access point*, pengguna mendapatkan notifikasi dan informasi konfigurasi *access point* tersebut dan dapat memilih untuk melakukan konfigurasi ulang atau bergabung ke dalam jaringan menggunakan konfigurasi yang diberikan oleh *access point.*

Metode PIN *Internal Registrar* dapat dianggap cukup aman karena membutuhkan akses kepada *Web Interface* dari *Access Point (registrar)* melalui perangkat yang sudah tergabung ke dalam jaringan (dan memiliki akses terhadap *web interface* dari *access point*) atau perangkat masukan lainnya yang terpasang pada *registrar* untuk mendaftarkan *enrolee*. Sedangkan metode *External Registrar* memiliki kelemahan yang akan dibahas lebih lanjut.

WPS PIN terdiri dari empat atau delapan angka. Umumnya, WPS PIN yang digunakan dan dispesifikasikan adalah delapan angka. Pada PIN yang terdiri dari delapan angka, struktur dari PIN adalah tujuh angka PIN dan angka terakhir sebagai *checksum* dari ketujuh angka di depannya seperti yang digambarkan pada Tabel II.1 Struktur PIN.

Tabel II.1 Struktur PIN

1	2	3	4	5	6	7	8
Bagian pertama PIN				Checksum			
				Bagian kedua PIN			

PIN yang hanya terdiri dari delapan angka, biasanya tercetak pada bagian belakang *access point* dan tidak ada kebutuhan lain untuk menginisiasi WPS mode *External Registrar* selain PIN membuat metode ini rawan mengalami serangan *brute force* [1]. Untuk melakukan *brute force* terhadap PIN yang terdiri dari delapan angka normalnya membutuhkan 10^8 (100.000.000) kali percobaan, akan tetapi karena proses validasi PIN, yang akan dibahas pada bagian berikutnya, memisahkan PIN menjadi dua bagian yang terdiri dari empat angka dan divalidasi terpisah mengurangi jumlah percobaan *brute force* menjadi $10^4 + 10^4$ (20.000) kali saja. Namun, angka terakhir dari PIN adalah *checksum* dari ketujuh angka didepannya sehingga dapat dihitung, keadaan ini memungkinkan *brute force* dapat dilakukan hanya dengan $10^4 + 10^3$ (11.000) percobaan saja.

III. Spesifikasi Protokol Kriptografi WPS

A. Proses WPS External Registrar

Dalam kasus WPS *External Registrar*, *registrar* dapat berupa sebuah perangkat lunak yang bertindak sebagai *registrar* contohnya Windows Connect Now untuk melakukan konfigurasi pada AP baru yang belum terkonfigurasi. Pada proses konfigurasi, perangkat lunak yang bertindak sebagai *registrar* akan meminta masukan dari pengguna diantaranya PIN dari perangkat AP, nama AP yang diinginkan, kunci pengaman WPA2 yang diinginkan pengguna atau dibangkitkan secara otomatis. Proses yang akan dilakukan oleh *registrar* adalah sebagai berikut [3].

1. AP mengirimkan rambu yang mengandung *Information Element* yang menyatakan bahwa AP mendukung *Wi-Fi Simple Configuration.*
2. *Registrar* mengirimkan *Wi-Fi Simple Configuration probe request* kepada AP dengan *request type* sebagai *registrar.*
3. AP mengirimkan *Wi-Fi Simple Configuration probe response* kepada *registrar* dengan *response type* sebagai AP.
4. Pengguna memasukkan PIN dari AP yang didapat dari membaca label yang tercetak pada AP atau pada *Web Interface* AP ke dalam *registrar*
5. *Registrar* menginisiasi sambungan 802.1x dengan nama "WFA-SimpleConfig-Registrar-1-0" sebagai *EAP-Response/Identity.*
6. AP dan *registrar* melakukan pertukaran pesan M1-M8 mengikuti panduan *Registration Protocol*. Pesan M7 memuat konfigurasi saat itu dari AP. Pesan M8 dapat memuat informasi pengaturan AP baru sesuai yang dimasukkan oleh pengguna pada *registrar*.
7. AP mengirimkan pesan EAP-Done, *registrar* mengirimkan EAP-ACK dan AP mengirimkan EAP-Failure yang menandakan berakhirnya sesi *Registration Protocol.*
8. *Registrar* dan AP melakukan pengaturan konfigurasi berdasarkan konfigurasi yang dikirimkan dari M7 atau M8. *Registrar* kemudian memutuskan sambungan dan melakukan sambungan ulang dengan AP sesuai dengan konfigurasi yang disepakati.

B. Spesifikasi Registration Protocol WPS

Pada bagian III.A telah disebutkan mengenai *Registration Protocol* untuk pertukaran pesan. Pesan dari *Registration Protocol* secara umum dibagi menjadi delapan bagian pesan yang disebut sebagai M1, M2, M3, M4, M5, M6, M7, dan M8. Urutan pengirim dan penerima pesan serta isi dari pesan M tergambar pada Tabel III.1 WSC *Registration Protocol* [3].

Tabel III.1 WSC *Registration Protocol* [3]

Arah Pesan	M	Isi Pesan
Enrollee → Registrar	M1	Version ‖ N1 ‖ Description ‖ PK_E
Enrollee ← Registrar	M2	Version ‖ N1 ‖ N2 ‖ Description ‖ PK_R
Enrollee → Registrar	M3	Version ‖ N2 ‖ E-Hash1 ‖ E-Hash2 ‖ $HMAC_{AuthKey}(M_2 \| M_3^*)$
Enrollee ← Registrar	M4	Version ‖ N1 ‖ R-Hash1 ‖ R-Hash2 ‖ $ENC_{KeyWrapKey}$(R-S1) ‖ $HMAC_{AuthKey}$ (M_3 ‖ M_4^*)
Enrollee → Registrar	M5	Version ‖ N2 ‖ $ENC_{KeyWrapKey}$(E-S1) ‖ $HMAC_{AuthKey}$ (M_4 ‖ M_5^*)
Enrollee ← Registrar	M6	Version ‖ N1 ‖ $ENC_{KeyWrapKey}$(R-S2) ‖ $HMAC_{AuthKey}$ (M_5 ‖ M_6^*)
Enrollee → Registrar	M7	Version ‖ N2‖ $ENC_{KeyWrapKey}$(E-S2 [‖ConfigData]) ‖ $HMAC_{AuthKey}$ (M_6 ‖ M_7^*)
Enrollee ← Registrar	M8	Version ‖ N1 ‖ [$ENC_{KeyWrapKey}$(ConfigData)] ‖ $HMAC_{AuthKey}$ (M_7 ‖ M_8^*)

Konvensi yang digunakan pada Tabel III.1 adalah sebagai berikut [3]:

- Simbol || melambangkan konkatenasi dari parameter-parameter untuk membentuk pesan.
- Huruf *subscript* dalam konteks fungsi kriptografik seperti HMAC_{Key} merujuk pada kunci yang digunakan pada fungsi tersebut.
- M_n^* adalah pesan M_n dengan tidak mengikutsertakan nilai dari HMAC-SHA-256.
- Version menunjukkan tipe dari pesan *Registration Protocol*.
- N1 adalah *nonce* 128-bit yang ditentukan oleh *Enrolee*. N1 baru harus dibangkitkan untuk setiap instans dari *Registration Protocol*. *Registrar* harus menggunakan nilai N1 yang diikutsertakan pada pesan M1 terbaru yang dikirimkan oleh *Enrolee*.
- N2 adalah nonce 128-bit yang ditentukan oleh *Registrar*. N2 baru harus dibangkitkan untuk setiap instans dari *Registration Protocol*. *Enrolee* harus menggunakan nilai N2 yang diikutsertakan pada pesan M2D/M2 terbaru yang dikirimkan oleh *Registrar*.
- Description memuat deskripsi yang dapat dibaca oleh manusia dari perangkat pengirim (UUID, pembuat, nomor model, MAC *address*, dll.) dan kemampuan perangkat seperti algoritma yang didukung, kanal I/O, peran pada *Registration Protocol*, dll.
- PK_E dan PK_R adalah kunci publik Diffie-Hellman untuk *Enrolee* dan *Registrar*.
- AuthKey adalah sebuah kunci otentikasi yang diturunkan dari rahasia Diffie-Hellman $g^{AB} \bmod p$, *nonce* dari N1 dan N2, dan MAC *address* dari *Enrolee*.
- E-Hash1, E-Hash2 adalah *pre-commitment* yang dibuat oleh *Enrolee* untuk membuktikan kepemilikan dari dua bagian PIN perangkatnya.
- R-Hash1, R-Hash2 adalah *pre-commitment* yang dibuat oleh *Registrar* untuk membuktikan kepemilikan dari dua bagian PIN dari *Enrolee*.
- ENCKeyWrapKey(…) Notasi ini menyatakan enkripsi simetris dari nilai dalam kurung menggunakan kunci KeyWrapKey. Algoritma enkripsi yang digunakan adalah AES-CBC per FIPS 197 dengan PKCS#5 v2.0 *padding*.
- R-S1, R-S2 adalah *nonce* rahasia 128-bit, bersama dengan R-Hash1 dan R-Hash2 dapat digunakan oleh *Enrolee* untuk melakukan konfirmasi akan pengetahuan *Registrar* terhadap kedua bagian PIN *Enrolee*.
- E-S1, E-S2 adalah *nonce* rahasia 128-bit, bersama dengan E-Hash1 dan E-Hash2 dapat digunakan oleh *Registrar* untuk melakukan konfirmasi akan pengetahuan *Enrolee* terhadap kedua bagian PIN *Enrolee*.
- $\text{HMAC}_{\text{AuthKey}}$(…) Notasi ini menandakan atribut dari *Authenticator* yang memuat nilai dalam kurung yang telah di *hash* menggunakan HMAC menggunakan kunci AuthKey. Fungi hash yang digunakan adalah HMAC-SHA-256 per FIPS 180-2 dan RFC-2104. Untuk mengurangi ukuran dari pesan, hanya 64 bit dari 256-bit hasil keluaran HMAC yang diikutsertakan dalam atribut *Authenticator*.
- ConfigData memuat konfigurasi jaringan nirkabel untuk *Enrolee*. Konfigurasi tambahan untuk jaringan dan aplikasi lainnya dapat juga disertakan dalam ConfigData. Meskipun ConfigData yang ditunjukkan disini selalu terenkripsi, enkripsi wajib hanya untuk *key*s dan *key bindings*. Enkripsi untuk data konfigurasi lainnya bersifat opsional.

C. *Algoritma KeyWrap*

Algoritma yang digunakan untuk melakukan fungsi key wrap untuk melindungi nonce rahasia dan ConfigData adalah sebagai berikut [3]:

1. Hitung KWA = 64 bit pertama dari $\text{HMAC}_{\text{AuthKey}}$(DataYangDienkripsi)
2. Bangkitkan IV acak 128-bit.
3. Hitung WrappedData = AES-Encrypt-$\text{CBC}_{\text{KeyWrapKey}}$(DataYangDienkripsi||KWA, IV)
4. IV diikutsertakan dalam WrappedData dalam atribut Encrypted Settings.

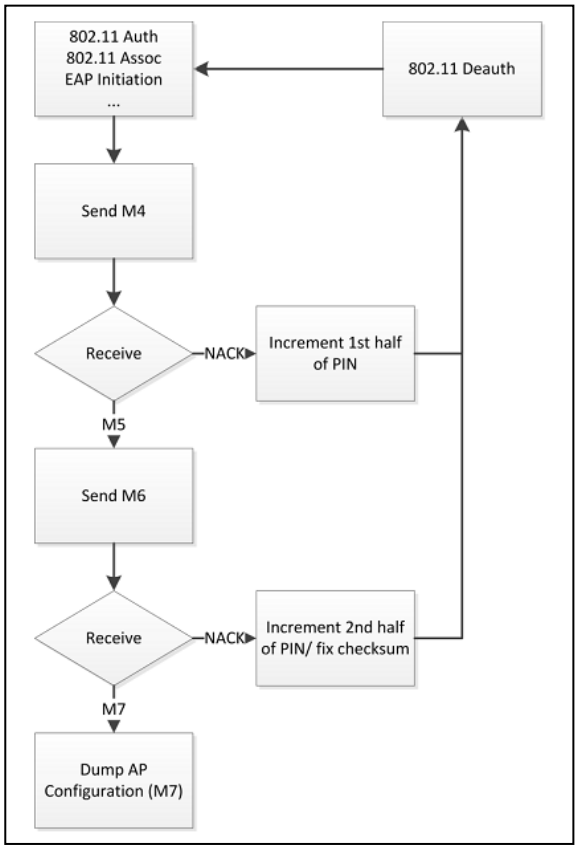
Untuk melakukan dekripsi digunakan algoritma sebagai berikut:

1. Data || KWA = AES-Decrypt-$\text{CBC}_{\text{KeyWrapKey}}$(WrappedData, IV)
2. Jika KWA = 64 bit pertama dari $\text{HMAC}_{\text{AuthKey}}$(Data) maka keluarkan Data, selain itu keluarkan "failure"

KWA adalah atribut Key Wrap Authenticator.

IV. SERANGAN TERHADAP PROTOKOL KRIPTOGRAFI WPS

Serangan terhadap protokol WPS *External Registrar* dapat dilakukan dengan metode *brute-force*. Pada bagian III, PIN dibagi menjadi dua dan divalidasi secara terpisah. Bagian pertama dari PIN dikirimkan pada pesan M4 berupa *hash*. Bagian kedua dari PIN dikirimkan pada pesan M6 juga berupa *hash*. Percobaan *brute force* dapat dilakukan dengan mencoba setiap kemungkinan dari PIN. Penyerang dapat mengetahui PIN yang dimasukkan salah jika penyerang mendapatkan pesan WSC_NACK yang menandakan kegagalan proses WPS setelah mengirimkan pesan M4. Ketika penyerang mendapat pesan M5 setelah mengirimkan M4, maka penyerang mengetahui bahwa bagian depan PIN yang dimasukkannya adalah benar dan melanjutkan percobaan dengan bagian belakang PIN sampai mendapatkan pesan M7. Setelah penyerang mendapatkan pesan M7, maka penyerang mendapatkan konfigurasi dari jaringan nirkabel beserta kombinasi delapan angka PIN yang benar yang kemudian PIN tersebut dapat digunakan di lain waktu sewaktu-waktu konfigurasi jaringan nirkabel yang didapatkan dari M7 berubah.



Gambar IV.1 Alur Serangan Terhadap Protokol WPS *External Registrar* [3]

Gambar IV.1 menunjukkan alur serangan *brute force* yang dapat dilakukan terhadap protokol WPS dengan mode *External Registrar*.

V. Analisis Pendeteksian Serangan

Bagian IV telah menjelaskan mengenai serangan yang mungkin dilakukan terhadap protokol kriptografi WPS dengan cara *brute force*. Cara paling mudah untuk menentukan terjadinya serangan terhadap protokol WPS adalah melihat karakteristik serangan yang mencoba memasukkan PIN yang ditambahkan satu setiap kali percobaan. Bagian dari PIN dikirimkan pada pesan M4 dan M6, tetapi PIN yang dikirimkan tidak pernah berupa *plain-text* melainkan *hash* dari bagian PIN seperti yang dijelaskan pada Bagian III dan IV. Oleh karena itu, pendeteksian tidak bisa dilakukan berdasarkan pesan M4 dan M6. Pesan lain yang dapat digunakan sebagai indikator terjadinya serangan terhadap protokol WPS ini adalah paket WSC_NACK yang tidak terenkripsi dan menandakan terjadinya kesalahan dalam proses WPS. Pesan WSC_NACK ini juga digunakan sebagai indikator penyerang dalam menentukan apakah penyerang memasukkan PIN yang salah.

Untuk memeriksa hipotesis penggunaan pesan WSC_NACK sebagai indikator maka akan dilakukan beberapa analisis dari hasil *packet capture* dengan program Wireshark untuk mengetahui paket / pesan yang terlibat dalam keadaan normal, dan dalam keadaan serangan.

Source	Destination	Protocol	Length	Info
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAPOL	79	Start
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	86	Request, Identity
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAPOL	79	Start
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	113	Response, Identity
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	511	Request, Expanded Type, WPS, M1
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	495	Response, Expanded Type, WPS, M2
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	495	Response, Expanded Type, WPS, M2
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	204	Request, Expanded Type, WPS, M3
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	274	Response, Expanded Type, WPS, M4
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	200	Request, Expanded Type, WPS, M5
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	202	Response, Expanded Type, WPS, M6
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	248	Request, Expanded Type, WPS, M7
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	250	Response, Expanded Type, WPS, M8
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	140	Request, Expanded Type, WPS, WSC_DONE
Tp-LinkT_13:2e:72	Cisco-Li_e7:61:c7	EAP	142	Response, Expanded Type, WPS, WSC_ACK
Cisco-Li_e7:61:c7	Tp-LinkT_13:2e:72	EAP	80	Failure

Gambar V.1 Hasil Wireshark pada WPS Normal yang Berhasil

Gambar V.1 menunjukkan paket-paket yang dideteksi oleh program Wireshark ketika proses WPS PIN berjalan secara normal dan berhasil. Program *registrar* yang digunakan pada kasus ini adalah program bawaan Windows 10 untuk melakukan pengaturan terhadap *access point* yang belum terkonfigurasi. Pada Gambar V.1 dapat dilihat bahwa tidak ada paket WSC_NACK yang dikirimkan oleh AP. Sumber yang berasal dari "TP-Link…" adalah *registrar* dan "Cisco…" adalah *Access Point* yang dikonfigurasi.

Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAPOL	44	Start
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAPOL	49	Start
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	86	Request, Identity
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	79	Response, Identity
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	84	Response, Identity
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	511	Request, Expanded Type, WPS, M1
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	427	Response, Expanded Type, WPS, M2
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	432	Response, Expanded Type, WPS, M2
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	204	Request, Expanded Type, WPS, M3
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	240	Response, Expanded Type, WPS, M4
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	245	Response, Expanded Type, WPS, M4
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	146	Request, Expanded Type, WPS, WSC_NACK
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	114	Response, Expanded Type, WPS, WSC_NACK
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	119	Response, Expanded Type, WPS, WSC_NACK
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAPOL	44	Start
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAPOL	49	Start
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	86	Request, Identity
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	79	Response, Identity
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	84	Response, Identity
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	511	Request, Expanded Type, WPS, M1
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	427	Response, Expanded Type, WPS, M2
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	432	Response, Expanded Type, WPS, M2
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	204	Request, Expanded Type, WPS, M3
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	240	Response, Expanded Type, WPS, M4
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	245	Response, Expanded Type, WPS, M4
Cisco-Li_e7:61:c7	Tp-LinkT_18:30:68	EAP	146	Request, Expanded Type, WPS, WSC_NACK
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	114	Response, Expanded Type, WPS, WSC_NACK
Tp-LinkT_18:30:68	Cisco-Li_e7:61:c7	EAP	119	Response, Expanded Type, WPS, WSC_NACK

Gambar V.2 Hasil Wireshark pada WPS dibawah Serangan

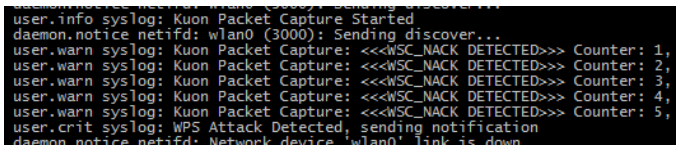
Gambar V.2 menunjukkan rangkaian paket pada saat terjadi serangan terhadap WPS. Dalam keadaan terserang paket WSC_NACK yang diterima sejumlah percobaan yang dilakukan oleh penyerang. Kesimpulan dari analisis paket diatas menyatakan bahwa paket WSC_NACK dapat dipakai sebagai indikator kegagalan. Sumber yang berasal dari "TP-Link…" adalah *registrar* penyerang dan "Cisco…" adalah *Access Point* yang sedang diserang. Kolom sebelah kiri adalah nama perangkat pengirim dan kolom sebelah kanan adalah nama perangkat penerima.

Karena percobaan secara *brute force* menggunakan program akan menghasilkan banyak percobaan yang salah, pendeteksian dapat dibatasi untuk mendeteksi sekian paket WSC_NACK untuk menyatakan bahwa terjadi serangan.

VI. Pendeteksian Serangan Sebagai Man-in-the-Middle

Implementasi dari pendeteksian jika dilakukan pada sisi *Access Point* akan sulit dikarenakan pada perangkat *Access Point* tidak bisa dilakukan instalasi program yang dibuat oleh pengguna. Oleh karena itu pendeteksian harus dilakukan sebagai pihak ketiga yaitu pihak yang mendengarkan secara pasif pertukaran pesan antara *registrar* dan *enrolee*. Karena paket WSC_NACK tidak dienkripsi maka pendeteksian berdasarkan paket WSC_NACK dapat dilakukan sebagai pihak ketiga yang mendengarkan pertukaran pesan.

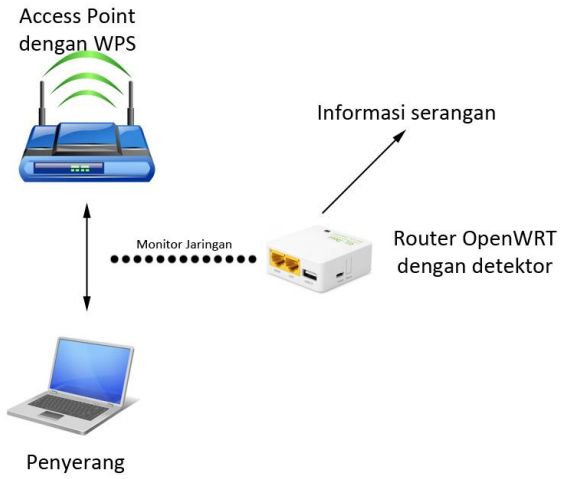
Sebagai pembuktian konsep dari usulan pendeteksian serangan sebagai *man-in-the-middle* telah dibangun sebuah *packet detector* dengan Bahasa C yang menggunakan pustaka *libpcap* pada sistem operasi berbasis linux untuk embedded yaitu OpenWRT versi 15.05.



Gambar VI.1 Program Pendeteksian

Gambar VI.1 menunjukkan hasil dari program pendeteksi yang telah dibangun dapat mendeteksi paket WSC_NACK yang dianggap sebagai serangan. Kode program dapat diakses pada tautan berikut https://github.com/michaelaw320/KuonWPSAttackDetector

Pengujian dilakukan langsung pada keadaan serangan nyata dengan *setup* sebagai berikut. Penyerang menggunakan sebuah desktop PC bersistem operasi Kali Linux dan *wireless adapter* TP-Link TL-WN722N untuk melakukan serangan terhadap sebuah *access point* tersertifikasi oleh *Wi-Fi Alliances* dan mendukung mode WPS yaitu Linksys WAG-120N. Solusi ditempatkan pada sistem operasi OpenWRT yang menempatkan *wireless adapter* miliknya dalam mode *monitor* yang memungkinkan mendengarkan seluruh pertukaran yang terjadi di kanal *Wi-Fi* tertentu. Penggambaran dari skenario pengujian tergambar pada Gambar VI.2.



Gambar VI.2 Gambaran *Setup* Pengujian

VII. Kesimpulan dan Saran

Kesimpulan yang dapat diperoleh adalah protokol kriptografi WPS sudah aman secara kriptografi akan tetapi beberapa kesalahan desain pada mode PIN *External Registrar* membuat protokol WPS mode PIN *External Registrar* dapat diserang.

Dengan menganalisis karakteristik dan spesifikasi detil mengenai WPS mode PIN *External Registrar* diusulkan sebuah metode untuk pendeteksian serangan terhadap protokol WPS. Metode yang diusulkan sudah diimplementasi dalam bentuk sebuah program pembuktian konsep yang dapat melakukan deteksi terhadap serangan yang terjadi pada protokol WPS melalui deteksi paket WSC_NACK.

VIII. Referensi

[1] A. Sadeghian, "Analysis of WPS Security in Wireless Access Points," dalam *6th International Conference on Security for Information Technology and Communications*, Bucharest, 2013.

[2] Microsoft, "A WINDOWS® RALLY™ SPECIFICATION," 8 Desember 2006. [Online]. Available: download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc. [Diakses 7 Mei 2016].

[3] Wi-Fi Alliances, "Wi-Fi Simple Configuration Technical Specification," 4 Agustus 2014. [Online]. Available: https://www.wi-fi.org/file/wi-fi-simple-configuration-technical-specification-v205. [Diakses 19 Mei 2016].

IX. PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Mei 2016

Michael Alexander Wangsa
13512046