PERANGKAT WIRO 1.0 SEBAGAI ALAT BANTU PROSES PENGUMPULAN INFORMASI WIFI

Gigih Supriyatno[1], Budi Siswanto[2]

[1,2]Badan Siber dan Sandi Negara
[1]Jln. Harsono RM no 70 Jakarta
[2]Jln. Muchtar Raya no 70 Bojongsari, Depok, Jawa Barat
e-mail: [1]gigih.supriyatno@bssn.go.id [2]budi.siswanto@bssn.go.id

Abstract

Information gathering activities are currently implemented with laptop equipment and external antennas. Such a device may cause suspicion that leads to personnel vulnerabilities in the field. This research will discuss about the design of equipment that is more flexible and small to support information gathering activities of wifi signal analysis by utilizing Rasberry Pi device as a replacement for laptop devices. The research method begins by describing how data retrieval works through wifi, how the Rasberry Pi works and then designing the device and the software system used. This design produces a special wifi signal gathering device pack 4-way handshake that has smaller dimensions, practical, avoid suspicion and able to operate automatically.

Keywords : *Wiro1.0, Wireless, Rasberry Pi, Signal*

1. Pendahuluan

Perkembangan teknologi informasi yang begitu pesat melahirkan tantangan baru bagi pengamanan dan pengumpulan informasi. Tahap pengumpulan informasi bisa diperoleh melalui berbagai sumber, salah satunya melalui jaringan internet. Salah satu transmisi informasi internet adalah menggunakan sinyal radio *wireless fidelity* (wifi).Tahap pengolahan informasi melalui wifi tersebut diantaranya dilakukan dengan memecah kode informasi yang tersandi didalamnya.

Kegiatan pengumpulan informasi yang berasal dari wifi disebut dengan kegiatan analisis sinyal wifi. Proses pelaksanaan pengumpulan informasi kegiatan tersebut menggunakan peralatan komputer portable (laptop) dan antena *wireless* eksternal. Kegiatan pengumpulan informasi tersebut dimaksudkan untuk mengambil paket data dari wifi yang berisi kata kunci (*password*) yang digunakan untuk mengakses wifi. Dari paket data tersebut tidak langsung dapat diperoleh *password* yang digunakan melainkan perlu dilakukan proses pemecahan *password* (*password cracking*).

Pelaksaanan kegiatan analisis sinyal wifi yang saat ini dilaksanakan masih terdapat beberapa kekurangan, diantaranya :

1. Penggunaan laptop dan antena eksternal dianggap tidak praktis karena akan terlihat mencurigakan ketika lokasi target wifi berada dilingkungan dengan pengamanan tinggi seperti instalasi militer dan gedung pemerintahan. Hal tersebut memunculkan ancaman keamanan dan keselamatan personil yang bertugas mengumpulkan informasi lapangan.
2. Proses pemecahan *password* dilakukan secara *remote* karena perangkat pemecah *password* memerlukan sumber daya (*resource*) yang besar untuk proses komputasi, sehingga tidak memungkinkan dikerjakan di lokasi kegiatan.
3. Tidak efisiennya waktu yang dipakai antara proses memulai kegiatan *password cracking* dengan kegiatan saat paket enkripsi ditemukan.

Adanya kekurangan dalam kegiatan analisis sinyal wifi tersebut, maka pada dipandang perlu melakukan penelitian tentang pemanfaatan perangkat mini-komputer sebagai solusi pengumpulan data dalam kegiatan operasi analisis sinyal wifi. Penelitian serupa pernah dilakukan oleh Al Barghuthi dkk [1] menggunakan *raspberry-pi* sebagai alat bantu untuk melakukan *penetration test* di lingkungan *smart* cities. Kegiatan *pentest* yang dilakukan bersifat umum menggunakan *tools* pentest seperti nessus, IBM appscan, dan OpenVAS. Hasil penelitian mereka menunjukkan bahwa penggunaan

raspberry-pi sama efektifnya dengan menggunakan laptop dan dengan kelebihan berupa *low cost, low energy*, dan lebih mudah untuk bergerak. Salah satu tujuan dari penelitian ini adalah menghasilkan sebuah perangkat portable yang secara otomatis akan melakukan proses analisis sinyal wifi sehingga dapat dipakai secara efektif di lingkungan yang tidak terkendali. WiRo 1.0 merupakan perangkat analisis sinyal yang memiliki dimensi yang efisien sehingga praktis dalam pergerakan secara mobile serta memiliki kemampuan berkomunikasi secara *real time* dengan perangkat pemecah *password*.

2. Telaah Literatur

Protokol Keamanan Wpa/Wpa2

WPA/WPA2 merupakan protokol pengamanan data yang digunakan dalam jaringan wifi. Sebelum data dikirimkan kepada klien (gadget, laptop, dan lainnya) data akan dienkripsi terlebih dahulu. WPA merujuk penggunaan model enkripsi *Temporal Key Integrity Protocol* (TKIP), sedangkan WPA2 merujuk pada model enkripsi *Counter Mode with CMC MAC Protocol* (CCMP)[3]. TKIP merupakan teknologi enkripsi yang dikembangkan dari teknologi enkripsi wifi WEP. WEP merupakan teknologi enkripsi wifi yang menggunakan algoritma RC4, namun dalam implementasinya WEP terdapat celah keamanan yang dapat di eksploitasi. TKIP menggunakan algoritma RC4 dengan beberapa perubahan. Dikarenakan TKIP merupakan pengembangan dari WEP dan tetap berbasiskan algoritma RC4, maka masih terdapat beberapa serangan yang serupa pada WEP yang masih bisa dilancarkan terhadap metode pengamanan TKIP ini[3].

CCMP diklaim sebagai algoritma yang paling aman saat ini pada pengamanan data wireless. CCMP memiliki fitur integritas data, autentikasi, dan kerahasiaan informasi. Berbeda dengan TKIP yang menggunakan algortima *stream cipher* RC4, CCMP menggunakan algoritma *block cipher* AES. Sebuah paket CCMP terdiri dari nomor paket, *header*, dan bagian terenkripsi (data dan MIC). Karena algoritma yang berbeda maka serangan yang umum bisa dilakukan pada WEP atau WPA tidak berlaku di WPA2[3].

Dari dua metode pengamanan diatas, terdapat pula dua standar autentikasi user yaitu 802.1X dan *Pre-Shared Key* (PSK). 802.1X menggunakan server sebagai validator user dan manajemen. kunci pada tiap user. Sedangkan metode PSK tidak memerlukan server tambahan karena setiap klien menggunakan kunci yang sama dari *passphrase* yang digunakan untuk mengakses jaringan wifi. Metode WPA/WPA2-PSK merupakan metode yang paling sering digunakan karena kemudahannya dan tidak memerlukan sumber daya tambahan.

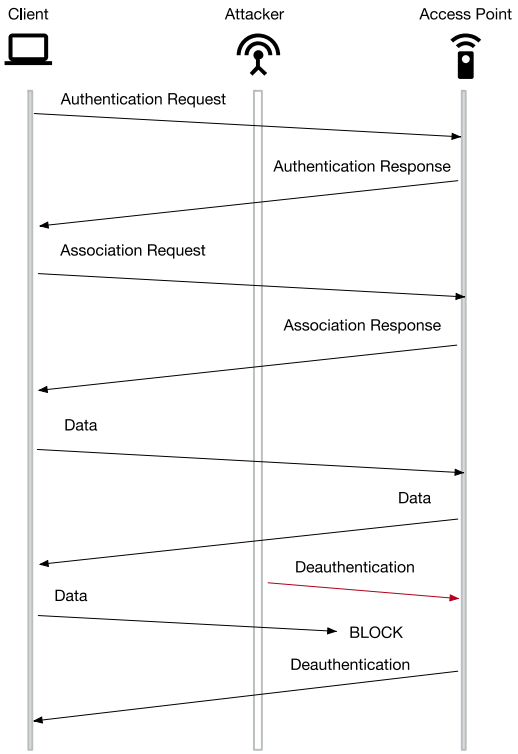
Ssh Public Key Authentication

Protokol komunikasi SSH (*Secure Shell*) merupakan protocol komunikasi *client – server* yang digunakan untuk melakukan remote session maupun file transfer (*Secure Copy Protocol*) dari klien ke server. Setiap kali data dikirim oleh komputer ke jaringan, SSH mengenkripsi secara otomatis. Saat data mencapai penerima yang dituju, SSH secara otomatis melakukan dekripsi (*unscrambles*). SSH menggunakan algoritma enkripsi 3DES, Blowfish, Twofish, CAST128, IDEA, dan ARCFOUR untuk mengenkripsi kontennya[9].Untuk proses autentikasi SSH menggunakan kriptografi kunci public (*public key cryptography*). Terdapat beberapa cara untuk melakukan autentikasi server dan klien diantaranya yang paling umum digunakan adalah *password based authentication* dan *public key authentication*[4]. Password based authentication meminta user memasukkan username dan password yang diijinkan terhubung ke server. Sedangkan untuk *public key authentication*, menggunakan sepasang kunci public dan kunci private. Sistem kerjanya server menyimpan kunci public klien yang sudah di otorisasi sehingga hanya klien yang memiliki kunci private yang dapat melakukan remote session ke server.

Teknik Serangan Deauthentication

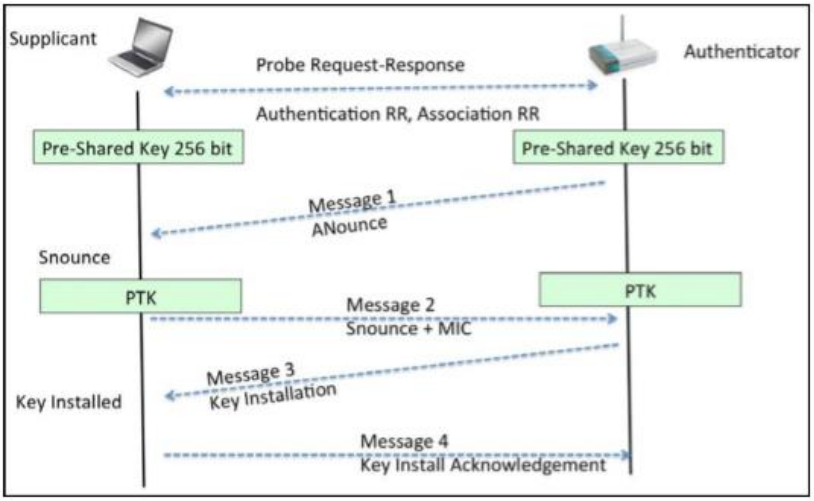
Serangan *deauthentication* merupakan jenis serangan pada jaringan wifi dengan cara mengirim paket *deauthentication* ke router/akses poin wifi. Disaat bersamaan penyerang mengirim paket ke klien dengan berpura-pura menjadi router wifi kemudian meminta klien melakukan re-auntentikasi ke akses point. Dari proses reautentikasi akan diperoleh *4-way handshake*. Sederhananya serangan ini memutus koneksi yang terjadi antara akses point dengan klien[5]. Serangan ini termasuk kedalam jenis serangan *denial of service (*DoS).

.



Gambar 1. Diagram proses serangan *deauthentication*

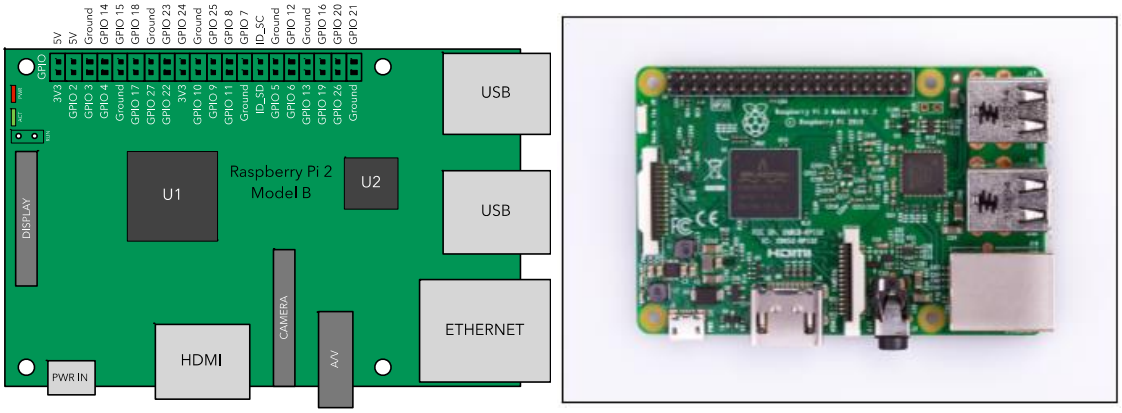
Serangan *deathentication* umumnya ditujukan untuk wifi dengan pengamanan WPA/WPA2-PSK. Dengan teknik serangan *deauthentication* akan diperoleh paket *4-way handshake*. Paket *4-way handshake* diperlukan karena paket tersebut berisi *pairwise transient key* (PTK) yang digunakan untuk mengenkripsi data yang ditransmisikan antara klien dan akses poin[7]. PTK di buat dari enam parameter yaitu PSK, nama SSID, *Authenticator Nounce*, *Supplicant Nounce*, *Access Point MAC Address*, dan wifi *Client MAC Address*. Paket *4-Way Handshake* dipakai sebagai bahan untuk proses *password cracking* sehingga menghasilkan passphrase akses poin[8].



Gambar 2. 4-*Way handshake*[5]

Rasberry Pi

Raspberry Pi merupakan sebuah SBC (*Single Board Computer*) atau mini komputer (PC) yang memiliki dimensi seukuran kartu kredit[5]. Dalam perkembangannya, Raspberry Pi kini telah mencapai generasi ke tiga. Sebagai mini komputer, Raspberry Pi memiliki beberapa spesifikasi yang mirip dengan sebuah komputer biasa seperti Micro SD sebagai media penyimpanan, *USB Port*, *Camera Interface*, *Ethernet port Wireless LAN*, Bluetooth, dan sebagainya. Raspberry Pi menggunakan arsitektur CPU ARMv8 quad core.



Gambar 3. Raspberry Pi

Mode Monitor 802.11x

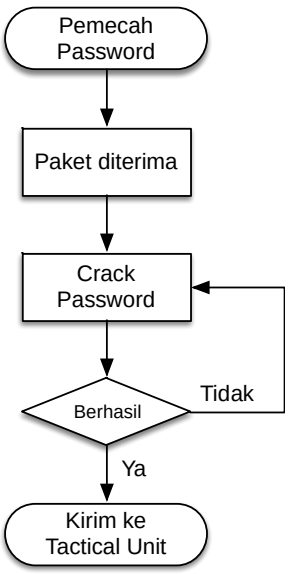
Sebuah perangkat *wireless* 802.11b/g/n umumnya memiliki 3 mode yaitu mode master, mode managed, dan mode monitor[2]. Pada mode master, perangkat *wireless* berlaku menjadi sebuah akses poin dengan identitas nama SSID. Sedangkan mode *managed* digunakan sebagai perangkat untuk mengakses jaringan SSID wifi. Mode monitor adalah mode yang membuat perangkat *wireless* dapat memonitor lalu lintas jaringan wifi[2]. Tidak semua perangkat wifi dapat menggunakan mode monitor. Hanya beberapa produsen chip yang bisa membuat perangkat *wireless* ke mode monitor seperti *atheros*, *broadcom*, *ralink*, *realtek* dan sebagainya. Mode monitor ini yang digunakan untuk melakukan pengumpulan informasi dari wifi.

3. Bisnis Proses Pengumpulan Informasi Wifi

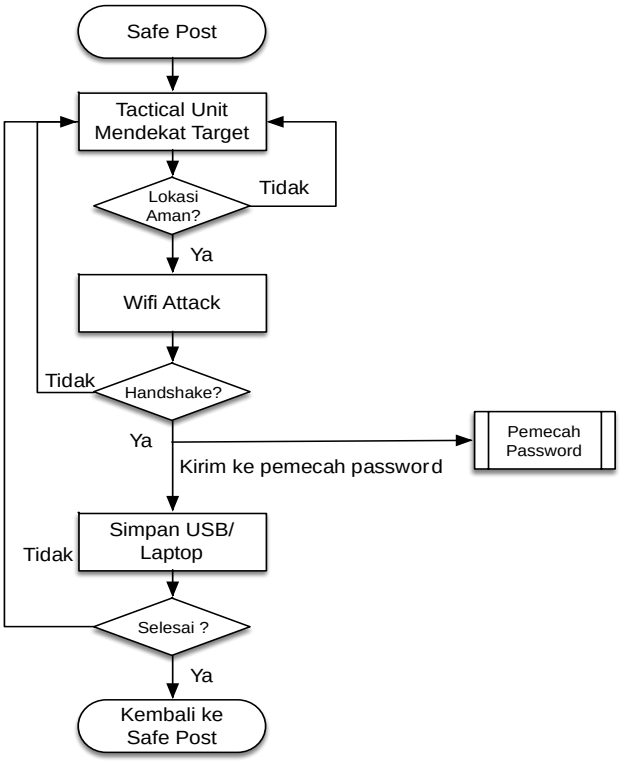
Pengumpulan informasi wifi dilakukan dengan menggunakan software *aireplay-ng*, *airmon-ng*, dan *airodump-ng*. Aplikasi software aplikasi tersebut berbasis *command text*. Tahapan yang dilakukan dalam pengumpulan informasi antara lain :

a. Memastikan perangkat utama saling terhubung;
b. Perangkat *wireless* di set menjadi mode monitor;
c. Menjalankan aplikasi *airodump-ng*;
d. Menjalankan aplikasi *aireplay-ng*;
e. Ketika diperoleh *4-way handshake*, disimpan dan dikirimkan ke perangkat *password cracking*.

Proses pengiriman *password cracking* dilakukan secara manual menggunakan email. Jika tidak memungkinkan, pengiriman dilakukan setelah kegiatan dilapangan selesai.



Gambar 4. Paket *handshake* masuk dalam proses *password crack*



Gambar 5. Diagram proses kegiatan analisis sinyal wifi

Kendala Pelaksanaan Pengumpulan Wifi

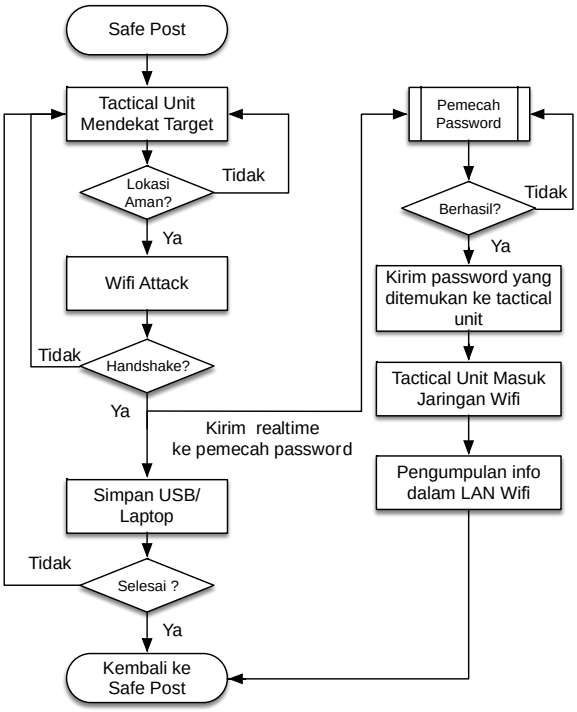
Dalam melakukan kegiatan analisis sinyal wifi terdapat beberapa kendala teknis yang dihadapi yaitu :

1. Peralatan utama analisis sinyal wifi memiliki dimensi yang tidak praktis ketika dibawa dengan cara berjalan kaki mendekati lokasi target.
2. Faktor keamanan personil akan terpengaruh karena akan terlihat mencurigakan ketika melakukan kegiatan dengan perangkat utama yang mencolok.
3. Terdapat waktu tunda (*delay*) ketika paket *handshake* diperoleh dari wifi target dengan proses *password cracking*. Proses pengiriman paket *handshake* tidak dilakukan secara *real time* dan perlu koordinasi dengan personil yang menangani bagian *password cracking* untuk siap menerima paket.
4. Proses pengiriman paket menggunakan email dari personil dilapangan ke personil yang menangani *password cracking*. Hal ini akan menjadi kendala ketika personil *password cracking* tidak langsung mengerjakan proses *password cracking* atau tidak ada transfer informasi dari personil satu ke personil lain pada bagian *password cracking*.
5. Ketika proses *password cracking* belum berhasil hingga kegiatan analisis sinyal wifi berakhir maka tidak akan diperoleh informasi lain dari jaringan wifi target seperti jumlah klien di jaringan LAN wifi, service yang ada di jaringan wifi, dan sebagainya.

4. Desain Perangkat Wiro 1.0

Kegiatan analisis sinyal wifi memiliki tujuan untuk memperoleh informasi melalui jaringan wifi, baik yang bersifat biasa maupun informasi yang bersifat rahasia. Untuk menghasilkan produk informasi yang lengkap dari kegiatan tersebut maka perlu mengoptimalisasikan setiap proses kegiatannya, seperti:

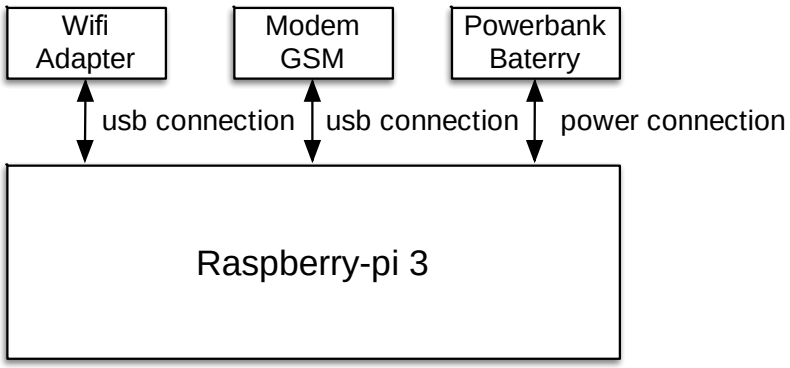
1. Data informasi yang dikumpulkan dari wifi target meliputi nama wifi, lokasi wifi, tipe pengamanan wifi, *password* wifi, jumlah klien di jaringan wifi, service yang ada dijaringan LAN wifi.
2. Proses *password crack* dilakukan secara *real time*. Ketika proses ini berhasil, *password* yang ditemukan dapat segera digunakan oleh personil dilapangan untuk melakukan pengumpulan informasi lebih lanjut.
3. Perangkat utama analisis sinyal harus praktis dan efisien sehingga pergerakan personil dilapangan dapat leluasa tanpa menimbulkan kecurigaan dari lingkungan target. Pergerakan dapat dilakukan dengan kendaraan maupun berjalan kaki.



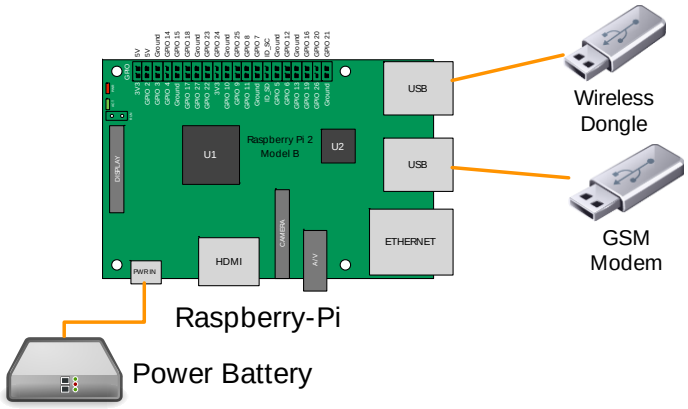
Gambar 6. Diagram proses perbaikan kegiatan analisis sinyal wifi

Desain Perangkat Wiro

Perangkat WiRo 1.0 (*Wireless Robot* versi 1.0) merupakan desain perangkat yang dibuat untuk melakukan tugas pengumpulan informasi dari wifi yang dapat berkomunikasi dengan perangkat *password cracking* secara *end-to-end device*. WiRo 1.0 didesain dengan dimensi minimalis menggunakan raspberry-pi3 sebagai mini-komputer dengan tujuan untuk mempermudah ketika dibawa bergerak (*mobile*). Perangkat ini juga didesain untuk melakukan pengambilan data (*4-way handshake*) dari wifi secara otomatis tanpa perlu bantuan personil untuk memasukkan perintah program pengambilan data wifi. Ketika paket *4-way handshake* ditemukan, WiRo 1.0 akan mengirim paket tersebut secara otomatis ke perangkat *password cracking* sehingga meminimalisir waktu jeda antara diperolehnya *handshake* dengan proses *password cracking*. Password yang telah di temukan pada proses *password cracking* dapat segera dikirim ke personil dilapangan. Perangkat WiRo 1.0 terdiri dari bagian *hardware* dan *software*. Bagian *hardware* memiliki spesifikasi fungsi yang serupa dengan perangkat analisis sinyal wifi, sedangkan *software* yang digunakan tetap sama seperti *airmonng, airodump-ng*, & *aireplay-ng.*



Gambar 8. Diagram blok fungsi komponen WiRo 1.0



Gambar 9. Komponen hardware WiRo 1.0

Perangkat Keras yang diperlukan Wiro 1.0 diantaranya :

a. Raspberry Pi 3 Model

Komponen ini berfungsi sebagai pengganti laptop atau PC dengan dimensi yang kecil. Raspberry Pi generasi ketiga memiliki spesifikasi teknis yang cukup memadai untuk menjalankan fungsi pengumpul sinyal wifi. Spesifikasi tersebut yaitu :

- 1.2GHz 64-bit quad-core ARMv8 CPU
- RAM 1 Gb
- 802.11n Wireless LAN internal
- Slot MicroSD
- Ethernet port

b. Wireless Adapter Eksternal

Wireless adapter yang dipakai harus mendukung mode monitor dan support dengan protocol 802.11 b/g/n yang bekerja pada frekuensi 2.4 Ghz. Mode monitor dibutuhkan untuk memonitor *traffic* sinyal *wireless* dan mengambil paket handshake darinya. Penelitian ini menggunakan perangkat *wireless* dari produk Alfa dengan spesifikasi sebagai berikut :

- Tipe AWUS051
- Support OS Windows dan Linux
- Standard protocol 802.11 a/b/g/n.

c. USB Modem GSM

Perangkat ini digunakan untuk menghubungkan perangkat WiRo 1.0 dengan perangkat *password cracking* melalui internet. Paket *handshake* dikirim melalui komunikasi SSH antara WiRo 1.0 dengan perangkat *password cracking*. Modem USB yang dipakai harus mendukung pada lingkungan sistem operasi Linux.

d. Powerbank battery

Perangkat ini berfungsi mendukung sumber daya bagi Raspberry Pi dalam operasionalnya. *Powerbank* yang digunakan sebaiknya menghasilkan output 2A 5V. Dalam penggunannya tidak ada spesifikasi khusus untuk perangkat ini namun disarankan menggunakan kapasitas baterai yang cukup besar minimal 16000mAh.

Perangkat Wiro 1.0 terdiri atas beberapa software *opensource* yang di program untuk bekerja secara otomatis ketika perangkat dinyalakan. Otomatisasi ini yang membedakan perangkat Wiro dengan perangkat analisis sinyal umum yang memerlukan operator untuk menjalankan perintah dan langkah – langkah operasional. Proses ini ditulis dalam sebuah *script bash* yang meliputi pekerjaan seperti *scanning* wifi yang ada di sekitar perangkat, melakukan serangan *deauth* untuk mengambil *handshake*, dan mengirim paket *handshake* ke mesin pemecah password. Berikut ini software *opensource* yang digunakan Wiro 1.0 diantaranya :

a. Aircrack-ng

Aircrack-ng merupakan aplikasi yang khusus dibuat untuk menguji keamanan dari jaringan wifi. Aplikasi ini memiliki fungsi yang mencakup *monitoring*, *attacking*, *testing* dan *cracking*. Pada perangkat WiRo fungsi-fungsi yang digunakan hanya fungsi monitoring dan attacking. Fungsi monitoring terdapat dalam subprogram *airmon-ng* dan *airodum-ng*, sedangkan fungsi *attacking* menggunakan subprogram *aireplay-ng*.

b. SCP (*Secure Copy Protocol*)

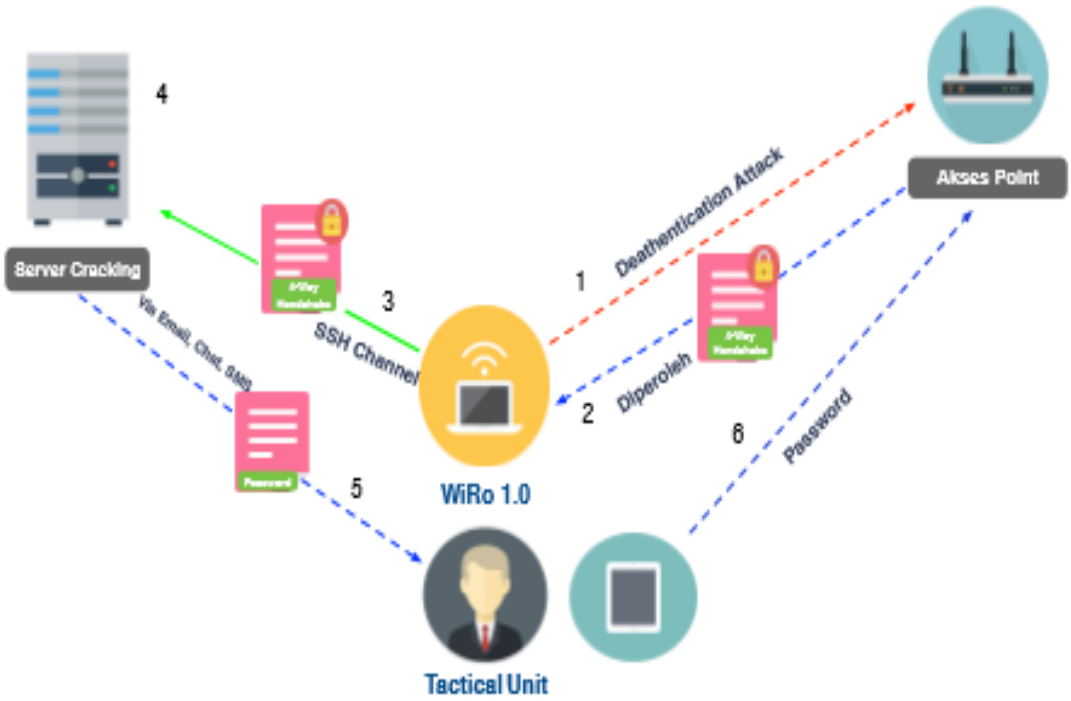
Program ini digunakan untuk mengirim file secara aman antara perangkat WiRo 1.0 dengan perangkat *password cracking*. SCP berbasis protokol SSH. Model authentikasi yang digunakan adalah *public key authentication* yaitu setiap kunci publik WiRo 1.0 disimpan pada *server cracking* sehingga hanya WiRo yang memiliki kunci privat yang bersesuaian yang dapat berkomunikasi dengan *server cracking.*

c. Sistem Operasi Unix-based

Perangkat WiRo menggunakan sistem operasi berbasis linux. Sistem linux digunakan karena dapat dikostumisasi sesuai dengan kebutuhan, terutama menyesuaikan dengan spesifikasi Raspberry Pi yang memiliki kemampuan terbatas bila dibandingkan dengan sebuah laptop. Sistem operasi linux yang disarankan adalah Kali Linux Rolling Versi 2016.2.

Proses kerja perangkat WiRo dilaksanakan sebagai berikut :

1. Perangkat WiRo dinyalakan pertama kali. Dalam tahap ini terdapat proses *boot* sistem operasi kemudian diikuti dengan menjalankan program *airmon-ng*, *airodum-ng*, *aireplay-ng*, *wvdial*, dan *ssh*. Program tersebut diaktifkan melalui *script bash* yang telah dilakukan konfigurasi untuk selalu aktif ketika OS pertama kali *boot*. *Wvdial* berfungsi sebagai program untuk mengaktifkan koneksi internet via USB modem.
2. Ketika WiRo mendeteksi sinyal wifi disekitarnya, perangkat akan mendata sinyal tersebut dan melakukan serangan *deauthentication*. Ketika serangan berhasil, WiRo akan mencatat ke sebuah log dan menyimpan paket *4-way handshake* dalam sebuah folder dengan nama *log_wifi*. Log berfungsi untuk mendata wifi apa saja yang berhasil diperoleh *4-way handshake* dan mencegah duplikasi serangan ke wifi tersebut. Proses tersebut dilakukan secara otomatis dengan menggunakan *script bash*.
3. Sebuah script lain akan memeriksa folder log_wifi yang berisi paket *4-way handshake* untuk dicatat dan kemudian di kirim ke perangkat *server cracking* melalu protokol SCP (SSH file transfer). Server akan mencatat dan menyimpan file yang dikirim.
4. Proses *password cracking* kemudian dikerjakan secara otomatis menggunakan *script* yang sudah dikonfigurasi. Apabila telah ditemukan *password* dari wifi target, server secara otomatis mengirim *password* ke unit tactical dilapangan via email. Pengiriman juga dapat dilakukan oleh personil yang menangani *server cracking.*
5. Personil dilapangan menggunakan password yang telah ditemukan dan menindaklanjuti informasi yang terdapat pada wifi target.



Gambar 10. Diagram kerja perangkat WiRo

5. Pembahasan dan Hasil

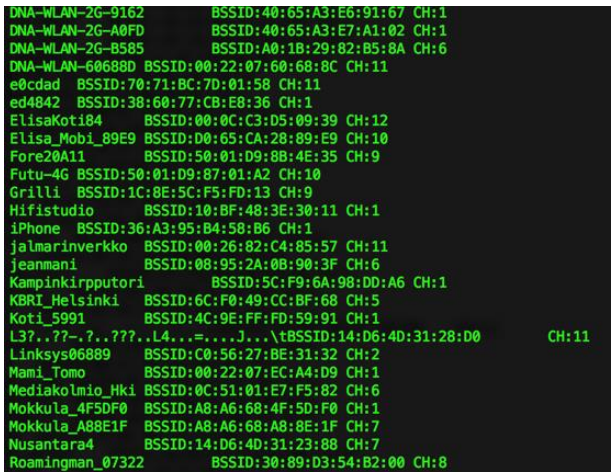
Perangkat wiro 1.0 memiliki kemampuan yang serupa dengan perangkat analisis wifi menggunakan laptop. Meskipun demikian perangkat ini tidak memiliki sumber daya komputasi yang sama besar dengan perangkat laptop. Fleksibilitas, mobilitas, dan otomatisasi merupakan keunggulan dari Wiro 1.0 sebagai perangkat analisis sinyal wifi. Wiro 1.0 tidak mempercepat proses komputasi pemecahan *password*, tetapi hanya mempercepat server untuk menerima input yang harus di kerjakan. Caranya adalah dengan mempersingkat proses pengambilan paket dan pengiriman ke server. Berikut beberapa pembahasan mengenai kinerja perangkat Wiro 1.0.

Scanning

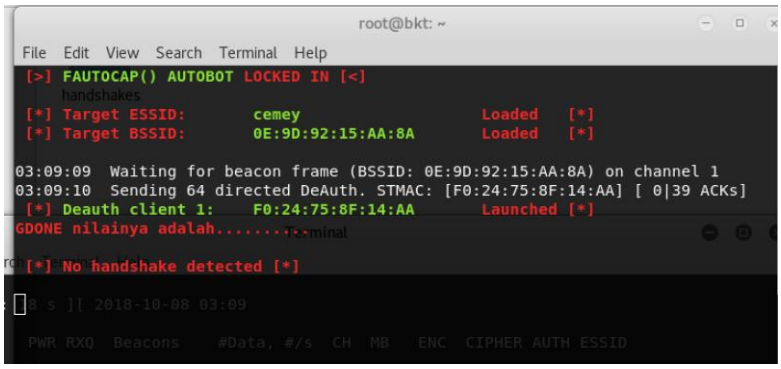
Pada tahap *scanning* jumlah akses poin yang di peroleh wiro 1.0 sama dengan laptop. Hal itu karena perangkat Wiro 1.0 menggunakan eksternal adapter wifi yang sama di pakai pada laptop sehingga hasil *scanning* tidak berbeda. Namun dengan dimensi yang lebih kecil dan tidak memerlukan interaksi operator, Wiro 1.0 dapat menjangkau daerah – daerah yang terlarang tanpa menimbulkan kecurigaan sekitar untuk mencari informasi wifi sehingga memperoleh hasil *scanning* yang lebih banyak. Gambar 11 merupakan contoh dari hasil scanning yang dilakukan Wiro 1.0.

Attack Wifi

Proses untuk memperoleh 4-way handshake dilakukan dengan *deauthentication attack*. Serangan ini menggunakan software aireplay-ng dan normalnya pekerjaan ini memerlukan operator untuk memilih dan memasukkan parameter – parameter akses poin yang menjadi target. Wiro 1.0 tidak memerlukan operator untuk tugas tersebut karena sudah di otomatisasi menggunakan script yang telah di buat. Setiap percobaan *deauthentication attack* yang berhasil akan diperoleh paket *4-way handshake* yang disimpan dalam sebuah folder. Apabila gagal memperoleh *4-way handshake* akan di ulang secara otomatis sebanyak 3 kali. Apabila tetap gagal maka akan pindah ke target selanjutnya. Gambar 12 merupakan contoh dari serangan yang dilakukan Wiro 1.0



Gambar 11. Contoh hasil scanning perangkat Wiro 1.0



Gambar 12. Serangan *deauthentication attack* secara otomatis

Komunikasi dengan Server Pemecah *Password*

Perangkat Wiro 1.0 melakukan komunikasi dengan server pemecah *password* melalui internet menggunakan scp. Apabila telah ditemukan paket *4-way handshake* yang dicatat dalam sebuah folder, maka secara otomatis file tersebut akan dikirim ke server pemecah *password*. Ukuran file yang dikirim tidak lebih dari 1 Mbyte. Server pemecah *password* harus memiliki IP public agar dapat di akses oleh Wiro 1.0. Kestabilan jaringan GSM sangat menentukan keberhasilan pengiriman paket *4-way handshake* ke server. Apabila terjadi kegagalan pengiriman maka secara otomatis akan di ulang sebanyak 3 kali percobaan pengiriman.

Power Supply

Perangkat Wiro 1.0 menggunakan *powerbank battery* sebagai sumber daya utama. *Raspberry-pi* memerlukan konsumsi listrik yang lebih sedikit (*low* energy) dibandingkan laptop. Dari hasil percobaan menggunakan *powerbank* dengan kapasitas 10.000 mAh, Wiro 1.0 dapat beroperasi lebih dari 5 jam. Jika dibandingkan dengan menggunakan laptop, penggunaan *raspberry-pi* lebih efektif ketika melakukan analisis sinyal wifi di area yang jauh dari sumber listrik.

Tabel Perbandingan Perangkat Analisis Wifi Umum dan WiRo 1.0

Parameter	**Perangkat Analisis Wifi Umum**	**Perangkat Wiro 1.0**
Komposisi Perangkat	▪ Laptop ▪ *Powersupply* Laptop ▪ *Wireless* eksternal 802.11 b/g/n	▪ *Raspberry Pi* ▪ *Wireless* Eksternal 802.11 b/g/n ▪ USB modem GSM *Powerbank* Battery
Dimensi	Perangkat seukuran laptop 13 inch atau dapat lebih besar	Perangkat seukuran kartu kredit
Proses pengambilan *handshake*	▪ Dilakukan secara manual maupun otomatis dengan script ▪ Kondisi layar laptop menyala	▪ Dilakukan secara otomatis dengan script ▪ Tidak memiliki layar internal, sehingga tidak terlihat proses yang dijalankan didalamnya
Pengiriman *handshake*	▪ Pengiriman paket *4-way handshake* dilakukan secara manual oleh personil ▪ Melalui email. ▪ Ada kemungkinan pengiriman dilakukan dengan jeda waktu yang besar dari pertama kali paket handshake didapat	▪ Pengiriman paket 4-way *handshake* dilakukan secara otomatis melalui saluran SSH. ▪ Jeda waktu antara saat pertama dapat *handshake* dengan pengiriman kecil karena prosesnya dilakukan dengan *script* yang akan memeriksa folder *log_wifi* terus menerus.
Keamanan	Personil dilapangan harus lebih hati – hati karena pengoperasian alat harus membuka layar laptop.	▪ Bentuk perangkat mini PC seperti powerbank ▪ Nilai ancaman terhadap personil dilapangan menurun dengan meminimalisir kecurigaan dari lingkungan sekitar. ▪ Pengoperasian alat cukup menekan tombol power on tanpa ada layar yang terlihat
Fleksibilitas	▪ Laptop memerlukan sumber daya listrik sehingga tidak fleksibel ketika dioperasikan lama. ▪ Perangkat utama memiliki beban dan dimensi yang lebih besar, sehingga kurang fleksibel ketika dibawa bergerak dengan berjalan kaki. ▪ Resiko rusak ketika guncangan lebih besar, khususnya *5* yang menggunakan pita magnetik	▪ WiRo 1.0 menggunakan sumber daya listrik dari baterai *powerbank*. Ketika digunakan untuk waktu yang lama, cukup dengan mempersiapkan *powerbank* dengan kapasitas yang besar atau dengan menyediakan beberapa power bank. ▪ Perangkat WiRo 1.0 memiliki beban dan dimensi yang ringan. Hanya powerbank yang memiliki beban paling besar diantara komponen hardware WiRo 1.0. ▪ Resiko rusak karena guncangan lebih kecil karena menggunakan penyimpanan berbentuk memori
Perkiraan Biaya	▪ Laptop 13 inch = ± Rp. 4.000.000 ▪ Eksternal wireless = ± Rp 300.000 ▪ Kerusakan perangkat PC membutuhkan biaya tinggi	▪ Raspberry Pi 3 model B = ± 600.000 ▪ Eksternal *wireless* = ± Rp. 300.000 ▪ Battery power bank = ± Rp. 200.000 ▪ Modem GSM & internet = ± Rp. 200.000 ▪ Kerusakan perangkat mini PC membutuhkan biaya rendah

Selain kelebihan yang telah di sebutkan, perangkat WiRo 1.0 juga memiliki beberapa kekurangan diantaranya :

1. Komunikasi WiRo 1.0 dengan perangkat *password cracking* sangat bergantung pada koneksi internet dari USB modem GSM. Jika mengalami gangguan pada sinyal provider yang digunakan maka komunikasi akan terganggu.
2. Tidak memiliki layar yang tertanam di *Raspberry pi* sehingga apabila terjadi gangguan program didalam WiRo 1.0 tidak dapat diketahui.
3. WiRo 1.0 menggunakan *Raspberry Pi* dengan spesifikasi terbatas. Ada kemungkinan perangkat menjadi tidak stabil ketika paket data yang disimpan melebihi kapasitas yang dimiliki *Raspberry Pi*.
4. Perangkat ini didesain hanya untuk menangkap paket *4-way handshake* sehingga belum dapat melakukan teknik serangan wifi lanjutan seperti *evil twin*, *social engineering attack*, *man in the middle*, dan sebagainya.
5. WiRo 1.0 belum dilengkapi dengan GPS yang dapat mencatat lokasi dari WiFi target.
6. WiRo 1.0 tidak menyimpan seluruh *traffic* data dari WiFi target hal ini berkaitan dengan keterbatasan media penyimpanan.
7. Perangkat ini tidak didesain untuk melakukan *password cracking* di tempat.

6. Kesimpulan

WiRo 1.0 merupakan prototipe perangkat untuk melakukan pengumpulan sinyal WiFi khusus untuk paket *4-way handshake* dari WiFi WPA/WPA2-PSK. WiRo 1.0 memiliki dimensi yang kecil dan cukup praktis untuk dibawa bergerak baik dengan kendaraan maupun berjalan kaki. Dengan dimensi yang kecil perangkat ini meminimalisir kecurigaan sehingga menurunkan ancaman bagi personil. WiRo 1.0 tidak mempercepat proses *password cracking*, namun dapat meringkas waktu antara pertama kali diperoleh paket *4-way handshake* dengan eksekusi proses *password cracking* sehingga lebih efisien. Proses yang dikerjakan oleh WiRo 1.0 semua berjalan otomatis sehingga memberikan kemudahan bagi personil. Biaya yang dibutuhkan untuk membuat WiRo 1.0 lebih murah dibandingkan dengan perangkat yang biasa digunakan

7. Rekomendasi

Beberapa rekomendasi pengembangan perangkat Wiro 1.0 adalah sebagai berikut :

1. WiRo 1.0 perlu dikembangkan kemampuannya sehingga dapat melakukan tugas lain seperti *man in the middle attack*, *evil twin*, *sniffing* dan sebagainya.
2. Perlu penelitian lebih lanjut terhadap peralatan dengan fungsi yang serupa WiRo agar dapat diperoleh perangkat yang lebih efektif dan efisien dilapangan.

Daftar Pustaka

[1] Al Barghuthi, dkk. *Evaluation of Portable Penetration Testing on Smart Cities Applications using Raspberry Pi III*. 2017. UEA, Dubai. The Fourth HCT Information Technology Trends (ITT 2017).

[2] Offensive Security Team. *Wireless Kungfu*. 2014.

[3] Caneill, M., & Gilis, Jean-Loup. Attacks against the wifi protocols WEP and WPA. 2010.

[4] Daniel J. Barrett and Richard E. Silverman. *SSH: The Secure Shell – The Definitive Guide*, https://docstore.mik.ua/orelly/networking_2ndEd/ssh/ch01_02.htm, (23 Mei 2017) pukul 14.00 WIB.

[5] Ramachandran, Vivek. *BakcTrack 5 Wireless Penetration Testing.* Mumbai, Packt Publishing Ltd, 2011.

[6] Rudito, A. Ramadhan, Anang Sularsa, & Mia Rosmiati. *Pembuatan Server Portable Berbasis Raspberry Pi Untuk Mendukung Pelaksanaan Assessment*. Telkom University, Fakultas Ilmu Terapan.

[7] Vanhoef, Mathy, & Piessens, Frank. *Advanced Wi-Fi Attacks Using Commodity Hardware*. Leuven, Departemen Of Computer Science.

[8] Wadhwa, Utkarsh. *Wireless Network Security: Tough Times*. India, Galgotias College.

[9] SSH Communications Security Corp, *Public Key Authentication for SSH*, https://www.ssh.com/ssh/public-key -authentication, (22 Mei 2017) pukul 20.00 WIB.