APAKAH WPA/WPA2 BENAR-BENAR AMAN? DEKRIPSI PAKET DATA TERENKRIPSI PADA WPA/WPA2

Siti Zaim
Lembaga Sandi Negara
e-mail : siti.zaim@lemsaneg.go.id

Abstract
WPA2 is considered as the most secure configuration for Wi-Fi network and widely used to secure private and enterprise Wi-Fi network. The early protocol, WEP uses RC4 stream cipher algorithm without key management and WPA uses Temporal Key Integrity Protocol (TKIP) with hash function to scramble the key, while WPA2 use Advanced Encryption Standard (AES) algorithm to encrypt data. One of parameter for generate encryption key in WPA/WPA2 is preshared key. In 2008, Beck and Tews have proposed a practical attack on WPA by exploiting the preshared key. In this paper, we propose exploitation preshared key to decrypt WPA/WPA2 encrypted data. As a result we propose some prevention and anticipation methods from users that utilize wireless network to protecting data during transmission in wireless network with WPA/WPA2 protocol.

***Keywords**: WPA/WPA2, Cryptography, Wireless, Preshared Key, Network Security.*

Abstrak
WPA2 dianggap sebagai konfigurasi paling aman pada jaringan Wi-Fi dan banyak digunakan untuk mengamankan jaringan pribadi maupun enterprise. Pendahulunya, WEP menggunakan algoritma RC4 tanpa menggunakan key management dan WPA menggunakan Temporal Key Integrity Protocol (TKIP) yang menggunakan algoritma hash untuk mengacak kunci, sedangkan WPA2 menggunakan algoritma Advanced Encryption Standard (AES) untuk enkripsi data. Salah satu parameter yang digunakan untuk membangkitkan kunci enkripsi pada WPA/WPA2 adalah preshared key .Tahun 2008, Beck dan Tews mengajukan sebuah serangan yang dapat diterapkan pada WPA dengan memanfaatkan preshared key. Pada paper ini akan dilakukan eksploitasi penggunaan preshared key untuk melakukan dekripsi paket data pada WPA/WPA2. Pada akhirnya dapat dilakukan upaya pencegahan dan antisipasi untuk melindungi data pada saat ditransmisikan menggunakan jaringan wireless dengan metode pengamanan WPA/WPA2 dari sisi pengguna yang memanfaatkan jaringan wireless.

***Kata Kunci** : WPA/WPA2, Kriptografi, Wireless, Preshared Key, Keamanan Jaringan.*

1. PENDAHULUAN

Perkembangan teknologi komunikasi memudahkan setiap orang untuk mendapatkan akses terhadap informasi. Salah satu media komunikasi yang berkembang saat ini memanfaatkan jaringan komunikasi internet berbasis wireless. Wi-Fi (*wireless fidelity*) adalah teknologi komunikasi *wireless* yang memanfaatkan gelombang radio dalam rangka menyediakan koneksi berkecepatan tinggi (IEEE, 2004). Wi-Fi semakin banyak digunakan karena mendukung mobilitas pengguna, mudah digunakan, dan tingkat interoperabilitasnya yang sangat tinggi terhadap aplikasi dan peralatan seperti konsol permainan video, jaringan rumah, PDA, telepon seluler, dan perangkat elektronik lainnya. Pada saat ini, Wi-Fi dapat dijumpai dengan mudah di tempat-tempat umum, seperti kafe, hotel, restoran, dan di kantor pemerintahan. Kemudahan akses terhadap jaringan wireless membuat setiap orang dapat memanfaatkannya setiap saat, sehingga aspek keamanan jaringan menjadi hal yang sangat penting.

IEEE mengeluarkan standar protokol enkripsi yang digunakan untuk keamanan pada *wireless* (*Wi-Fi*), yaitu IEEE 802.11 yang merekomendasikan metode enkripsi yang dapat digunakan untuk pengamanan *wireless access point* (*Wired Equivalent Privacy*) WEP dan *Wi-Fi Protected Access* (WPA). WPA muncul karena adanya beberapa permasalahan yang signifkan pada WEP, antara lain ukuran kunci yang kecil, yaitu 5 karakter untuk WEP-64 dan 13 karakter untuk WEP-128, tidak terdapat *key management*, menggunakan algoritma RC4 yang sudah banyak ditemukan kelemahan didalamnya, dan mudah untuk memalsukan pesan otentikasi pada WEP (Lehembre).

WPA memiliki 2 (dua) mode otentikasi yang dapat dipilih, yaitu mode personal yang menggunakan *preshared key* untuk otentikasi dan mode *enterprise* yang menggunakan RADIUS server

untuk otentikasi *client*. Penggunaan *preshared key* dapat dieksploitasi oleh pihak yang tidak berhak untuk mendapatkan *passphrase* dari *Wirelss Access Point* (WAP). *Passphrase* merupakan salah satu parameter yang diperlukan untuk dapat mendekripsi pesan yang terenkripsi pada jaringan *wireless* dengan mode pengamanan WPA2. Pada makalah ini akan dijelaskan metode untuk dekripsi paket data terenkripsi pada WPA/WPA2 yang menggunakan *preshared key* (PSK) untuk otentikasi *client*, serta upaya pencegahan yang dapat dilakukan dari sisi pengguna agar data yang penting tetap terlindungi.

2. TINJAUAN PUSTAKA

Sejak dikeluarkannya WPA/WPA2 oleh IEEE sebagai standar untuk pengamanan jaringan *wireless* IEEE 80211, telah muncul banyak serangan baik dari sisi algoritma maupun dari sisi implementasi yang bersifat praktis. Beberapa penelitian yang telah dilakukan terkait dengan keamanan pada jaringan dengan menggunakan metode otentikasi WPA/WPA2 antara lain sebagai berikut.

Tabel 2. Penelitian Terkait Serangan pada WPA/WPA2

rPeneliti	Deskripsi Serangan
Beck, November 2008	*Practical Attack Against WEP and WPA*
Daniel, 2009	*WPA Password Cracking: Parallel Processing on the Cell BE (Master Thesis)*
Tomcsanyi, April 2010	*Taking a Different Approach to Attack WPA2-AES, or the born of the CCMP Known Plaintext Attack*
Caneil et al, Desember 2010	*Attacks Against the Wi-Fi Protocol WEP and WPA*
Johnson, 2010	*Wireless Preshared Key Cracking (WPA, WPA2)*
Patterson et al, Maret 2014	*Plaintext Recovery Attack Against WPA/TKIP.*
Ohigashi et al	*A Practical Message Falsification Attack on WPA*
Cassola et.al	*A practical, Targeted , and Stealthy Attack Against WPA Enterprise Authentication*

3. METODE PENELITIAN

Metodologi yang digunakan dalam pembahasan makalah adalah studi kasus. Analisa data monitoring jaringan dilakukan dengan menggunakan cara manual dengan menggunakan Wireshark. Komputer yang dijadikan target monitoring data menggunakan koneksi jaringan wireless dengan data sebagai berikut.

Tabel 2. Data IP Target Monitoring

Komponen	IP
IP Address	192.168.0.101
Subnet Mask	255.255.255.0
Gateway	192.168.0.1

Dalam melakukan analisis data monitoring digunakan *tools* berikut.

Tabel 3. Tools Analisis Data

Tools	Keterangan
Wireshark	Digunakan monitoring data, analisis data dan *live decrypt* paket data
Aircrack-ng	Digunakan untuk melakukan *dictionary attack passphrase* WPA/WPA2
Airdecap-ng	Digunakan untuk dekripsi paket data secara *offline*

4. HASIL DAN PEMBAHASAN

4.1. WPA/WPA2

Wi-Fi *Protected Access* (WPA/WPA2) merupakan standar keamanan jaringan *wireless* yang keluarkan untuk mengatasi kelemahan yang ada pada sistem pengamanan pendahulunya, yaitu *Wired Equivalent Privacy* (WEP). Terdapat 2 (dua) metode otentikasi yang dapat dipilih pada WPA/WPA2 yaitu *Temporal Key Integrity Protocol* (TKIP) dan AES-CCMP.

WPA menggunakan *Temporal Key Integrity Protocol* (TKIP) yang merupakan modifikasi dari WEP. Perubahan yang dilakukan oleh TKIP adalah sebagai berikut:

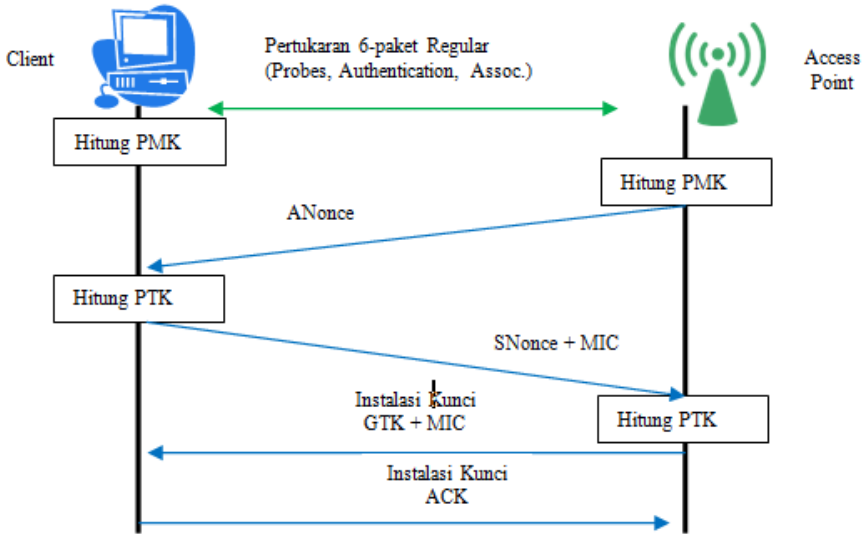
- *Message integrity cod*e (MIC) ditambahkan pada setiap paket sebelum fragmentasi sehingga dapat mencegah terjadinya serangan seperti *fragmentation* atau *chopchop,* dan melindungi *plaintext fragment* untuk mencegah adanya modifikasi *source/destination address* pada paket. TKIP juga tidak menggunakan algoritma SHA1MAC atau MD5HMAC untuk menghitung MIC karena membutuhkan waktu perhitungan CPU yang lama. TKIP didesain untuk dapat digunakan pada hardware yang sudah ada dengan menginstal *firmware*. Oleh karena itu dikembangkan algoritma baru, Michael yang lebih cepat dibandingkan SHA1MAC. MIC digunakan untuk mendeteksi error pada data baik yang terjadi pada saat pengiriman maupun karena perubahan untuk tujuan tertentu.
- Untuk mencegah *attacker* menebak *checksum*, atau serangan terhadap algoritma Michael dengan bantuan *wireless station*, TKIP hanya mengijinkan sedikit pesan dengan *checksum* CRC32 benar, tapi MIC tidak benar. Jika terdapat lebih dari 2 pesan diterima oleh station dalam satu menit, TKIP akan *disable* untuk satu menit dan disarankan untuk melakukan renegosiasi kunci.
- *Packet sequence counter* (TSC) digunakan untuk mencegah *replay attack*. Jika paket yang diterima habis, paket akan di drop oleh station penerima. Hal tersebut dapat mencegah semua jenis *injection attack* seperti ARP *injection attack*.
- Pada WEP, paket diubah hanya pada 3 byte pertama tiap paket kunci yang merupakan *initialization vector* (IV), TKIP mengubah setiap paket kunci setelah setiap paket tunggal. *Key mixing function* digunakan untuk menggenerate paket kunci didesain untuk mengabaikan nilai yang dapat digunakan untuk FMS *attack*.
- Meskipun banyak perbaikan yang dilakukan TKIP, TKIP tetap menggunakan algoritma RC4. Namun demikian, meskipun menggunakan *secret key* yang sama, ukuran TKIP adalah 128 bit, lebih panjang dari yang digunakan pada WEP yaitu 40 bit.
- WPA TKIP membutuhkan otentikasi *user*, sedangkan WEP hanya menggunakan MAC address yang mudah untuk dipalsukan di diketahui dan dipecahkan. WPA menggunakan *Extensible Authentication Protocol* (EAP) yang menggunakan enkripsi kunci publik untuk mengautentikasi *user* di jaringan. EAP bekerja pada layer data link dan melibatkan pengiriman dan penerimaan permintaan dan respons antara pihak-pihak dalam jaringan untuk melakukan otentikasi. EAP mengatur otentikasi *user* dengan *username/password*, sertifikat digital, dan *smart card* atau kredensial apapun yang nyaman digunakan pada saat membangun jaringan.

WPA2 menggunakan metode AES-CCMP. AES dengan *counter mode* (CCMP) digunakan untuk mengenkripsi traffic pada jaringan dan melindungi integritas data. AES menggantikan algoritma RC4 dan Michael serta menyediakan tingkat keamanan yang lebih tinggi. AES-CCMP digunakan pada WPA2 dan menggunakan framework 802.1X/EAP sebagai bagian dari infrastruktur yang memastikan *mutual authentication* yang terpusat dan manajemen kunci yang dinamis. WPA2 didesain unntuk mengamankan semua versi device 802.11 meliputi 802.11a/b/g, *multiband* dan *multimode*. Yang membedakan dengan WPA adalah WPA2 menggunakan *mixed mode* yang mendukung perangkat dengan WPA dan WPA2 pada *wireless network* yang sama. Terdapat perbedaan yang signifikan antara WPA dan WPA2, yaitu WPA2 menggunakan AES untuk enkripsi data, sedangkan WPA menggunakan TKIP. Penggunaan AES membuat upaya untuk memecahkan WPA2 membutuhkan kemampuan dan sumber daya yang sangat besar. Efektifitas penggunaan AES tidak dapat diperdebatkan, waktu untuk memecahkan AES menggunakan *bruteforce attack* dengan mikroprocessor 1 juta dolar dan panjang kunci 128 bit adalah 2.20×10^{17} tahun dan dengan panjang kunci 192 bit meningkat 10^{36} (Daniel, 2009).

WPA dan WPA2 memiliki dua mode yang dapat dipilih, yaitu mode *enterprise* dan mode personal. Mode enterprise menggunakan RADIUS server untuk mengotentikasi *client*. *Passphrase*

digenerate oleh RADIUS server dan dikirim secara aman ke *client* dengan didahului otentikasi dari *client* dan bersifat dinamis. Mode personal menggunakan *Preshared key* (PSK)/*passphrase* untuk mengotentikasi *client*. *Passphrase* disetting pada sisi *client*/AP (*Access Point*) dan bersifat statis. *Passphrase* memiliki ukuran 8 – 63 karakter. Setelah dilakukan pengaturan *passphrase* pada sisi *Client* dan AP selanjutnya akan terjadi perhitungan sebagai berikut:

- *Passphrase* digunakan untuk menghitung PSK/PMK(*Pairwise Master Key*)
  PSK/PMK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
  4096 menunjukkan jumlah hashing yang dilakukan terhadap *passphrase* dan 256 adalah panjang output PSK yaitu 256 bit atau 32 karakter heksa.
- PMK kemudian digunakan untuk menghitung PTK (*Pairwise Transient Key*) menggunakan 4-*way WPA handshake* antara *client* dan AP.
  PTK = PRF-X (PMK, *Pairwise key expansion*, Min (macAP, macSTA) || Max (macAP, macSTA) || Min (ANonce, SNonce) || max (ANonce, SNonce)).
  PTK berukuran 512 bit untuk TKIP dan 384 bit untuk CCMP. PTK terdiri empat *temporary key* yaitu *Key Confirmation Key* (KCK) 128 bit (bit 0-127) digunakan untuk mengotentikasi MIC selama *four way handshake* dan *Group Key Handshake*, *Key Encryption Key* (KEK) 128 bit (bit 128-255) digunakan untuk memastikan kerahasiaan selama *four way handshake* dan *Group Key Handshake*, *Temporal Encryption Key* (TEK) 128 bit (bit 256-383) digunakan untuk enkripsi data, dan TMK 2-64 bit (bit 384-447 untuk TMK1 dan bit 448-511 untuk TKM2 yang digunakan untuk otentikasi data pada TKIP dengan Michael *algorithm*.
  PTK tersebut selanjutnya digunakan mengenkripsi *traffic* data *user*. PMK yang dihasilkan oleh *client* dan AP harus sama, jika tidak, maka komunikasi yang dilakukan gagal. Proses 4 way handshake ditunjukkan pada Gambar 1.



Gambar 1. Mekanisme *four way handshake* pada WPA/WPA2

Access Point (AP) menghitung random number ANonce dan *supplicat/client* (STA) juga menghitung *random number* SNonce. AP mengirimkan ANonce ke *client*, sehingga *client* memiliki PMK, ANonce, dan SNonce. *Client* menghitung PTK dengan parameter yang telah dimiliki yaitu PMK, ANonce, dan SNonce. *Client* ju ga menghitung *Message Integrity Check* (MIC) dengan PTK yang dihasilkan. *Client* mengirimkan SNonce dan MIC ke AP. Selanjutnya AP menghitung PTK dengan mengetahui PMK, ANonce, dan SNonce. AP juga menghitung MIC dan membandingkan dengan MIC yang diterima dari *Client*. AP mengirimkan pesan dan MIC ke *client* dan *client* dapat melakukan verifikasi dengan tahapan yang sama. Proses 4 *way handshake* berhasil jika AP dan *Client* menghasilkan MIC yang sama.

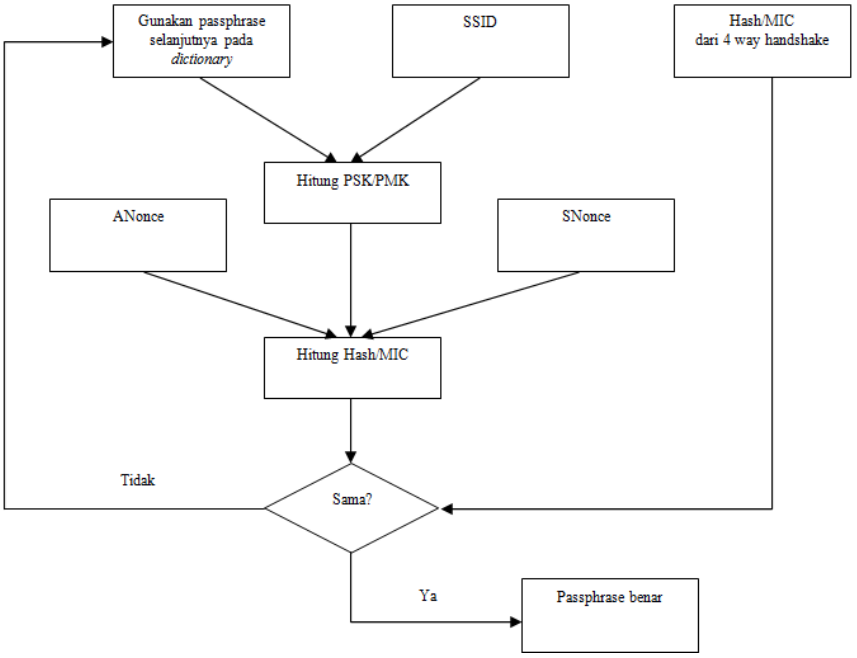
Yang menjadi catatan pada saat proses *four way handshake* terjadi adalah PMK tidak benar-benar ditransmisikan, tetapi digenerate pada AP dan *Client* dan digunakan sebagai input untuk menghitung PTK. Setiap *Client* akan menggenerate PTK yang berbeda, karena setiap *Client* memiliki SNonce yang berbeda sehingga suatu *client* tidak dapat mendekripsi traffic *client* lain dengan PTK yang dimiliki. *Client* dan AP saling mengotentikasi dan mengenkripsi data dengan PTK yang telah dibuat.

Proses *four way handshake* akan menghasilkan 4 EAPOL *(Extensible Authentication Protocol over* LAN) yang memungkinkan untuk mengkonfirmasi pengetahuan *client* tentang PMK, mendapatkan PTK yang baru, menginstal kunci enkripsi dan integriti, mengenkripsi transport pada GTK dan mengkonfirmasi pemilihan *cipher*.

4.2. Serangan pada *Preshared Key*

Meskipun WPA/WPA2 telah menambahkan perbaikan terhadap parameter yang digunakan, namun tetap ada bagian yang dapat dieksploitasi, yaitu penggunakan *preshared key.* PTK diperoleh dari PMK dengan melalui proses 4 *way handshake*, dan informasi yang dibutuhkan dikirim secara plaintext. Oleh karena itu, kekuatan PTK hanya bergantung pada PMK yang artinya bergantung pada kekuatan *passphrase* yang digunakan. *Passphrase* dapat diperoleh dengan beberapa metode antara lain dengan *man in the middle attack*, misalnya dengan tools Linset. Sedangkan *offline*, serangan dapat dilakukan dengan *dictrionary/bruteforce attack* dengan memanfaatkan EAPOL yang diperoleh pada saat *four way handshake* antara AP dan *Client* terjadi, atau dengan melakukan *social engineering*.

Pada saat *four way handshake* terjadi, ada 4 pesan EAPOL yang berisi parameter-parameter yang diperlukan untuk melakukan *cracking* guna mendapatkan *passphrase* yang digunakan untuk otentikasi. Keberhasilan metode *dictionary attack* bergantung pada *dictionary* yang digunakan. Mekanisme untuk mendapatkan passphrase dengan menggunakan *dictionary attack* dapat digambarkan sebagai berikut.



Gambar 2. Mekanisme *dictionary attack passphrase* pada WPA/WPA2

4.3. Dekripsi Paket Data pada WPA/WPA2

Traffic komunikasi antara *client* dan *wireless access point* pada WPA2 dienkripsi menggunakan algoritma AES dengan mode counter yang secara teori sangat kuat dan dibutuhkan sumber daya yang sangat besar untuk dapat memecahkannya. Namun implementasi algoritma tersebut pada WPA2 memiliki kelemahan, yaitu kunci yang digunakan untuk mengenkripsi menggunakan parameter *passphrase*, sehingga dengan mendapatkan *passphrase* akan dapat mendekripsi *traffic* data pada WPA2. Untuk dapat melakukan melakukan dekripsi data pada WPA ada beberapa hal yang harus dipenuhi, yaitu:

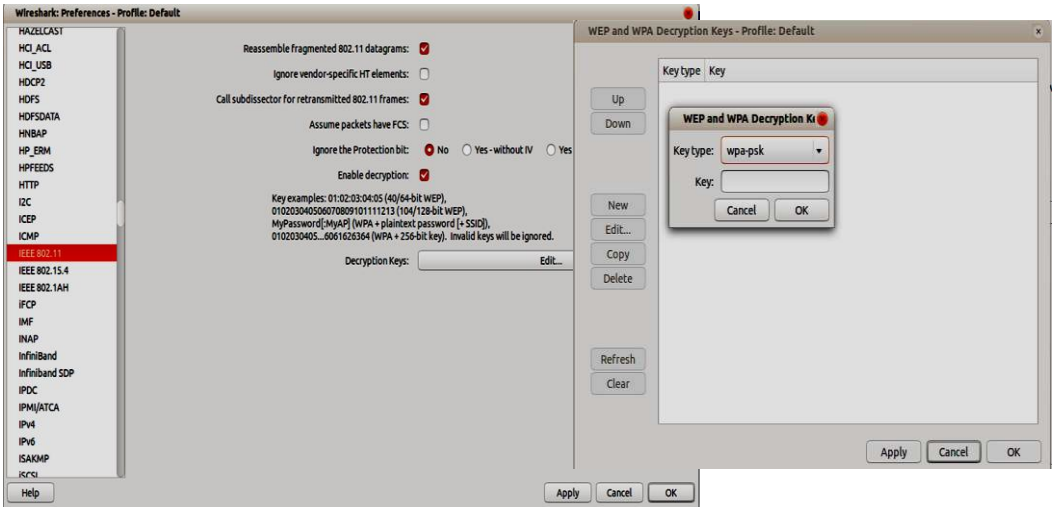
- Mengetahui *Service Set Identifier* (SSID) dan *passphrase* WAP
  SSID merupakan nama dari *access point*. SSID dan WAP akan digunakan untuk menghitung *preshared key* (PSK/PMK)
- Memiliki *handshake message* dari *client* yang menjadi target

Setiap *client* memiliki kunci enkripsi yang unik, yang dipengaruhi oleh *nonce Client* (SNonce). Untuk dapat mendekripsi *traffic* paket data *client* tertentu harus mendapatkan SNonce yang terdapat pada *handshake client* dan WAP. Handshake message yang diperlukan untuk dapat mendekripsi adalah EAPOL 1 dan EAPOL 2.

- Untuk mendekripsi secara *offline*, file capture harus memuat *handshake message* (EAPOL) dari *client* target

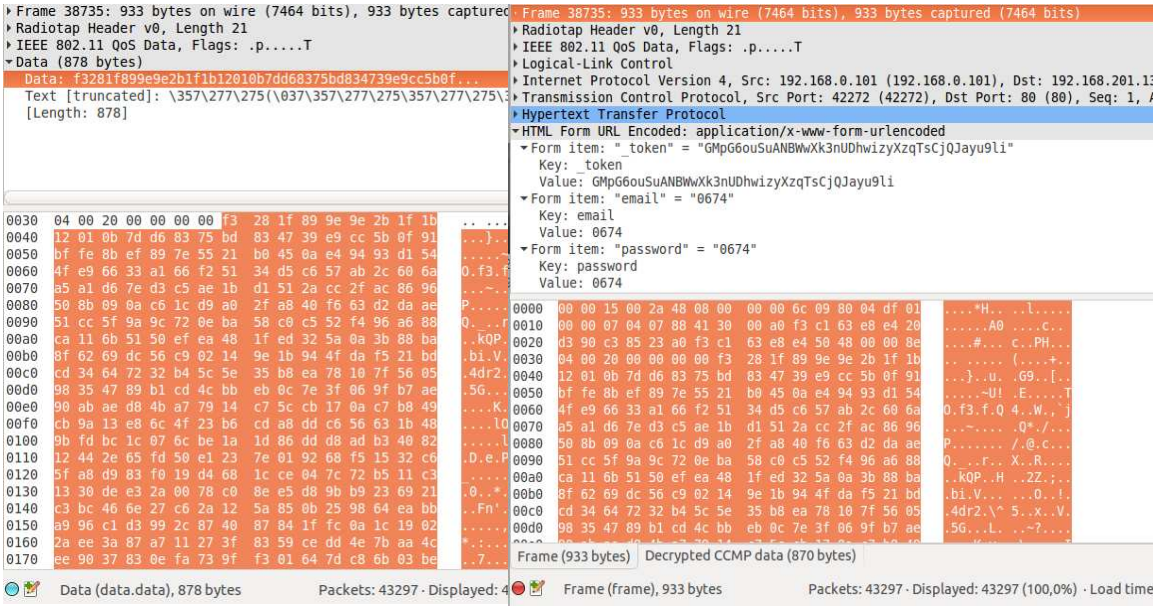
Terdapat dua metode yang dapat digunakan untuk melakukan dekripsi data pada WPA/WPA2, yaitu metode *live decrypt* dan *offline decrypt*. *Live decrypt* dilakukan pada saat proses *capturing* data berlangsung, dengan menggunakan tool Wireshark. Proses *live decrypt* dilakukan dengan tahapan berikut:

- Aktifkan mode monitoring pada *interface* jaringan yang dipilih
  Mode monitoring akan memungkinkan interface dapat menerima traffic yang ada pada jaringan tanpa terkoneksi dengan jaringan target.
- Pilih AP yang menjadi target
  Sebelum melakukan monitoring dilakukan scanning terhadap seluruh WAP yang ada, setelah ditemukan AP yang akan menjadi target, filter MAC AP tersebut pada wireshark.
- Lakukan *dump* menggunakan wireshark dengan mode *promiscuous*
  Mode promiscuous akan memungkinkan interface dapat menerima traffic dari dan ditujukan untuk interface lain.
- Lakukan deotentikasi *client* untuk memperoleh handshake
  Deotentikasi dilakukan untuk medapatkan *handshake message* dari *client* target.
- Cek kelengkapan handshake message yang diperoleh untuk *client* target
  Handshake message yang diperlukan untuk dapat mendekripsi pesan adalah EAPOL 1 dan EAPOL 2. Jika EAPOL 1 dan 2 belum berhasil dicapture, maka perlu dilakukan deotentikasi ulang.
- Enable fitur dekripsi pada wireshark, dan masukkan preshared key
  Wireshark menyediakan fitur dekripsi untuk protokol IEEE 802.11. Untuk memasukkan kunci dapat dilakukan dengan dua cara yaitu pertama memilih tipe wpa-pwd dan menginputkan passphrase:ssid atau wpa-psk dengan memasukkan presharedkey berupa 32 digit heksadesimal.
- Lakukan monitoring proses dump data, jika EAPOL *client* sudah lengkap, maka traffic *client* tersebut sudah dapat didekripsi.



Gambar 3. Fitur Dekripsi WPA pada Wireshark

Berikut contoh perbandingan data yang terenkripsi dengan data yang telah didekripsi.



(a) (b)

Gambar 4. Perbandingan paket data terenkripsi (a) dan paket data didekripsi (b)

Penggunaan wireshark untuk dekripsi paket terenkripsi pada WPA/WPA2 memiliki keterbatasan yaitu tidak dapat menyimpan file yang sudah didekripsi dalam ekstensi file capture (*.pcap,*.cap). Sehingga jika file tersebut dibuka menggunakan software lain akan masih tetap terenkripsi sehingga belum bisa dilakukan analisis data lebih lanjut dengan menggunakan tools lain.

Airdecap-ng merupakan salah satu tool yang dapat digunakan untuk menedekripsi file yang terenkripsi secara *offline*. Dekripsi traffic *client* tertentu dapat dilakukan jika file capture memuat handshake message dari *client* target. Parameter yang diperlukan untuk dapat mendekripsi dengan menggunakan airdecap-ng adalah SSID dan passphrase atau nilai *preshared key*. Hasil dekripsi dengan menggunakan airdecap-ng berupa file dengan ekstensi *.cap sehingga dapat dianalisis lebih lanjut dengan menggunakan software analisis paket data seperti Wireshark dan Network Miner.

(a) (b)

Gambar 5. Proses dekripsi *offline* dengan Airdecap-ng (a) dan file hasil dekripsi (b)

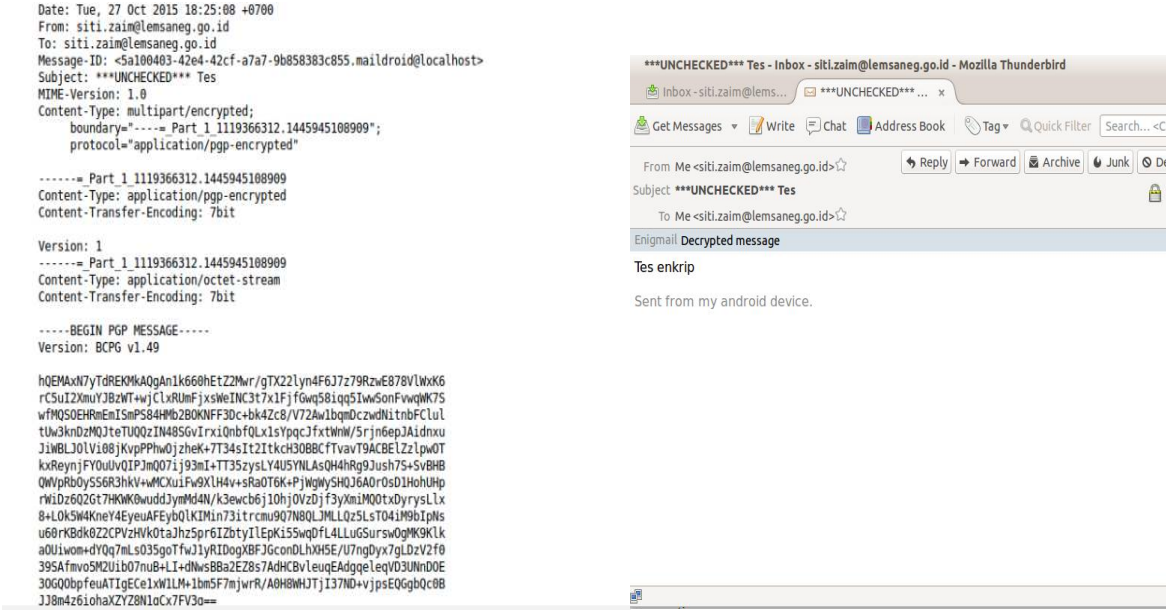
4.4. Upaya Pencegahan

Tidak ada sistem yang benar-benar aman, begitu juga dengan penggunaan WPA/WPA2 untuk pengamanan jaringan *wireless*. Oleh sebab itu, sebagai pengguna yang memanfaatkan jaringan *wireless* sudah menjadi suatu keharusan untuk melakukan upaya untuk melindungi data yang dinilai penting.

Upaya pencegahan dapat dilihat dari dua sisi, yaitu penyedia jaringan dan pengguna. Dari sisi pengguna yang memanfaatkan jaringan wireless, upaya pencegahan dan antisipasi dilakukan salah satunya dengan meningkatkan aspek keamanan, terutama ketika memanfaatkan jaringan internet menggunakan *wireless access point* publik. Sebagai pengguna *wireless access point* seharusnya setiap pribadi dapat menggunakannya jaringan wireless yang terproteksi dengan WPA/WPA2 dengan bijak dan meningkatkan kesadaran keamanan (*security awareness*) antara lain dengan hal-hal berikut:

- Tidak mengakses hal-hal yang memuat rahasia pribadi atau bersifat penting di *access point* umum meskipun terproteksi dengan mode WPA/WPA2.
- Melindungi data-data yang akan ditransmisikan dengan menggunakan enkripsi data/kriptografi, misalnya *Secure Socket Layer* (SSL), *Pretty Good Privacy* (PGP), atau enkripsi data *offline*, sehingga meskipun data dapat didump, masih membutuhkan sumber daya yang lebih besar untuk dapat mendekripsinya.
- Mengakses *website/url* yang terenkripsi untuk sharing data/dokumen. Enkripsi website ditunjukkan dengan huruf 's' pada https**.** Beberapa website hanya i/https pada halaman login, sedangkan halaman lain tidak, sehingga seluruh data pada akun tersebut rentan terhadap berbagai serangan. Untuk itu pastikan semua halaman website dienkripsi (https).
- Mempelajari dan memahami tentang keamanan pada jaringan Wi-Fi untuk memahami keamanan dan kerawanannya sehingga dpat melakukan upaya pencegahan dini dan dapat melindungi data yang penting.

Pretty Good Privacy (PGP) merupakan salah satu metode enkripsi yang menggunakan sistem kriptografi kunci publik (*public key cryptography*). Pihak yang akan berkomunikasi harus bertukar kunci publik untuk dapat mengirimkan pesan. Pesan dienkripsi dengan menggunakan kunci publik, dan akan didekripsi dengan menggunakan kunci privat. Salah satu pemanfaatan PGP adalah untuk enkripsi email. Pasangan kunci publik dan privat digenerate dengan menggunakan algoritma RSA dengan menggunakan parameter yang disebut *passphrase*. Untuk dapat mendekripsi pesan yang dienkripsi dengan PGP, pengguna harus memasukkan *passphrase* yang digunakan untuk membangkitkan pasangan kunci publik dan privat. Berikut contoh pesan yang dienkripsi dengan menggunakan PGP.



(a) (b)

Gambar 6. Pesan dienkripsi dengan PGP (a) dan pesan hasil dekripsi (b)

5. KESIMPULAN

Perkembangan teknologi komunikasi berbasis internet berbasis wireless (Wi-Fi) memudahkan orang untuk mendapatkan informasi secara aktual dan dapat melakukan sharing data tanpa dibatasi ruang

dan waktu. Namun dibalik ketersediaan dan kemudahan dalam mengakses internet berbasis Wi-Fi muncul ancaman terhadap keamanan data yang ditransmisikan. Kelemahan/kekurangan suatu parameter pada suatu protokol dapat menjadi celah dan mempengaruhi keamanan protokol secara keseluruhan. Seperti pada WPA2, meskipun menggunakan algoritma enkripsi yang sangat kuat, yaitu *Advanced Encryption Standard* (AES), namun karena mekanisme *handshake* memiliki kelemahan pada *preshared key* yang digunakan, maka dekripsi paket data yang ditransmisikan menjadi mudah dilakukan. Oleh sebab itu, kesadaran akan pentingnya keamanan informasi (*security awareness*) menjadi hal yang wajib. Dengan adanya kesadaran akan pentingnya keamanan informasi maka setiap pihak dapat melindungi datanya terutama pada saat ditransmisikan pada jaringan internet berbasis *wireless* (Wi-Fi) meskipun menggunakan mode pengamanan WPA2.

DAFTAR PUSTAKA

Ahmad, M. 2010. *WPA Too!,* submitted in Defcon 18 2010.

Beck,M., Tews, E. 2008. *Practical Attack Against WEP and WPA*.

Caneill,M., Gilis, J. 2010. *Attack against the Wi-Fi Protocol WEP and WPA*.

Daniel, M. 2009. *WPA Password Cracking: Parallel Processing on the Cell BE.* Master Thesis, Applied Signal Processing and Implementation: Aalborg University.

Johnson, D. 2010. *Wireless Pre-Shared Key Cracking (WPA,WPA2)* v 1.0.

Katz,F. 2005. *WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?*

Lehembre, G. *Wi-Fi Security – WEP, WPA and WPA2*.

Tews,E. 2007. *Attack on the WEP Protocol*. Diploma Thesis, Fachbereich Informatik: TU Darmstadt.

Tomcsanyi, D., Lueg, L. 2010. *Taking a Different Aproach to Attack WPA2-AES, or born of the CCMP known-plain-text Attack.*

Vanhoef,M., Piessens,P. 2013. *Practical Verification of WPA-TKIP Vulnerabilities*, Asia CCS 13, ACM 978-14503-1767-2/13/05.

IEEE. 2004. IEEE 80211i-2004, *Amandement* 6: *Medium Access Control (MAC) Security Enhancements,* IEEE Standard.

Airdecap-ng, http://www.aircrack-ng.org/doku.php?id=airdecap-ng, diakes 2 September 2015.

How to Decrypt 802.11, https://wiki.wireshark.org/HowToDecrypt802.11 diakses 1 September 2015.

My Security Awareness. Tips for Using Publi Wi-Fi Network. http://www.mysecurityawareness.com/article.php?article=333&title=tips-for-using-public-wi-fi-networks#.Vef0C7O1mkA diakses 3 September 2015.