BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Enkripsi telepon suara pada VoIP sangat berguna untuk mengamankan komunikasi telepon. Selain keamanan, telepon suara VoIP harus menjaga kualitas data suara pada telepon supaya suara tersebut dapat didengar dengan jelas, data suara tidak rusak/cacat. Penulis menganalisis keamanan serta pengaruh perubahan *Codec* terhadap telepon suara terenkripsi pada VoIP. Telepon suara VoIP terenkripsi dilakukan dari *client* 401 ke *client* 9001, dan komunikasi VoIP tanpa enkripsi dilakukan dari *softphone* SIPSorcery ke *client* 402 dan *client* 9002. Analisis tersebut menggunakan aplikasi Wireshark. Kemudian, telepon terenkripsi tersebut juga diuji keamanannya menggunakan aplikasi Cain and Abel dengan penyerangan APR *Poisoning*. Pada pengujian ini juga digunakanlah beberapa *Codec audio* yaitu *Alaw*, *Ulaw*, G722, dan G729. Hasil pengujian serta analisis keamanan dan *quality of service* dari sistem telepon suara VoIP FreePBX adalah sebagai berikut:

a. Percobaan pengujian keamanan telepon suara VoIP terenkripsi dengan TLS dan SRTP dengan penyerang yang dilakukan sebanyak 4 kali (dengan masing-masing telepon suara VoIP terenkripsi menggunakan *codec Alaw, Ulaw,* G722, dan G729).
    1) Untuk semua telepon VoIP, *cipher suite* yang digunakan oleh protokol TLS adalah TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. Protokol TLS mempunyai bahan tertentu dan kemudian diolah dalam proses *handshake* TLS supaya menciptakan kunci enkripsi.
    2) *Softphone* dan server VoIP melakukan protokol persinyalan VoIP dengan SIP. Mereka saling berkirim *handshake SIP call flow.* Ketika protokol SIP ingin memberikan informasi media VoIP kepada target, dia menggunakan protokol SDP. Protokol ini akan membantu komunikasi VoIP supaya bisa terenkripsi dengan SRTP.
    3) Untuk semua telepon VoIP, *cipher suite* yang digunakan oleh protokol SRTP adalah AES_CM_128_HMAC_SHA1_80.

Protokol SRTP melakukan enkripsi *RTP stream* dari hasil komunikasi antara *softphone* dengan server VoIP dengan *cipher suite* dan bahan-bahan tertentu.

4) Gambar spektrum RTP audio telepon VoIP dari telepon suara VoIP terenkripsi, telepon suara VoIP terenkripsi dengan serangan, dan suara rekaman dari VoIP client menunjukkan perbedaan yang sangat signifikan.
5) Hasil pengujian keamanan telepon suara VoIP FreePBX terenkripsi adalah sebagai berikut.
   i. Untuk telepon suara VoIP terenkripsi yang menggunakan *codec Alaw*, *Ulaw*, G722, dan G729:

      TLS Sertifikat Server didapat, Informasi SIP dan *cipher suite* dari SDP berhasil didapat, data suara RTP didapat dan tidak bisa di-*decrypt*, login *client* 401 normal, *client* 401 memanggil tujuan = normal, telepon suara di *client* 401 = normal, Panggilan berakhir di *client* 401 = normal, login *client* 9001 normal, *client* 9001 memanggil tujuan = normal, telepon suara di *client* 9001 = normal, file rekaman dari *SoftPhone* MicroSIP pada *client* 401 bisa dibuka dan ada suara.
   ii. Untuk telepon suara VoIP terenkripsi yang menggunakan *codec Alaw* dan *Ulaw*:

      9001 tidak bisa *End Call* setelah 401 mengakhiri panggilan, *file* rekaman dari *SoftPhone* MicroSIP dari *client* 9001 rusak.
   iii. Untuk telepon suara VoIP terenkripsi yang menggunakan *codec* G722 dan G729:

      Panggilan berakhir pada *client* 9001 Normal, file rekaman dari *SoftPhone* MicroSIP pada *client* 9001 bisa dibuka dan ada suara.

Hasil serangan dengan ARP *poisoning* pada telepon suara VoIP terenkripsi menurut aspek keamanan dalam kriptografi menunjukkan bahwa sistem VoIP FreePBX ada kegagalan dalam melaksanakan 3 aspek keamanan kriptografi yaitu *confidentiality, non-repudiation,* dan *authentication*. Tetapi, ada satu aspek keamanan kriptografi yang berhasil dilaksanakan yaitu *data integrity.*

b. Setelah pengujian ini dilakukan di aplikasi SoftPhone MicroSIP dan server FreePBX dengan *codec audio* berbeda-beda, hasil *Quality of Service* dari telepon suara terenkripsi ialah sangat baik dan tidak ada penurunan kualitas yang signifikan. *Delta*, *jitter*, dan *packet loss* yang dinilai sangat baik ini berdasarkan standar QoS TIPHON. Nilai *Delta* terbaik terdapat pada *Codec Ulaw*, Nilai *packet loss* terbaik terdapat pada *Codec Ulaw*, dan Nilai *jitter* terbaik terdapat pada *Codec Alaw*. Setelah telepon VoIP diserang dengan APR *poisoning*, ada penurunan kualitas QoS. Meskipun ada penurunan kualitas, suara dari *Client* 1 sampai dan masih terdengar jelas oleh *Client* 2. Kenaikan dan penurunan kualitas QoS pada telepon suara VoIP terenkripsi bisa dilihat pada tabel berikut ini.

Codec	***Delta***		***Jitter***		***Packet Loss***	
G729	↓	49.91%	↓	381.77%	↑	53.13%
Alaw	↓	21.43%	↓	767.97%	↓	5.56%
Ulaw	↓	104.12%	↓	601.14%	↓	181.82%
G722	↓	9.34%	↓	235.49%	↓	180.00%

Tabel 5.1 Presentase Kenaikan dan Penurunan QoS

Pengaruh pengubahan *Codec* pada telepon suara terenkripsi dan pada telepon yang diserang tidak memberikan perbedaan nilai *Quality of Service* yang jauh. Pengubahan *codec* diperlukan jika sistem VoIP tersebut ingin menggunakan *codec* dengan kecepatan tertentu dan *bitrate* tertentu.

c. Hasil analisis komunikasi VoIP FreePBX yang menggunakan enkripsi dengan melihat alur komunikasi VoIP yang tertulis pada *log file softphone* MicroSIP dan tanpa menggunakan enkripsi dengan melihat hasil *output* berupa *live log* komunikasi VoIP dalam aplikasi *command line* .NET C# SIPSorcery. Kedua komunikasi tersebut menggunakan protokol SIP sebagai protokol persinyalan telepon VoIP dan protokol SDP sebagai protokol penunjang informasi sesi multimedia telepon VoIP. Dalam telepon terenkripsi, pada protokol SDP terdapat atribut *crypto* yang berisikan *cipher suite* dan *key*, serta terdapat atribut *media* yang berisikan RTP/SAVP (menandakan VoIP ini menggunakan RTP yang terenkripsi). Dalam telepon terenkripsi, pada protokol SDP tidak terdapat atribut *crypto* dan terdapat atribut *media* yang berisikan RTP/AVP

(menandakan VoIP ini menggunakan RTP yang tidak terenkripsi dan hanya menggunakan protokol non-kriptografi atau UDP).

5.2 Saran

Adapun saran untuk penelitian ini kedepannya adalah sebagai berikut:

a. Ketika pengujian keamanan telepon pada telepon suara VoIP terenkripsi sebaiknya menggunakan banyak metode Enkripsi. Seperti ZRTP, VPN, dll.
b. *Codec* yang digunakan dalam penelitian ini sebaiknya diperbanyak. Banyak sekali *Codec audio* yang digunakan oleh banyak *SoftPhone* seperti G726, G723, SPEEX, SPEEX16, SPEEX32, SIREN7, ADPCM, SILK8, SILK12, SILK16, SILK24, G719, SLIN, SLIN12, SLIN16, SLIN24, SLIN32, SLIN44, SLIN48, SLIN96, SLIN192, LPC10, TESTLAW, NONE, GSM, ILBC, OPUS, *CODEC*2, SIREN14.
c. Untuk aplikasi *SoftPhone* SIPSorcery yang hanya bisa *attender blind call,* tambahkan pada aplikasi supaya bisa telepon suara ke telepon tanpa enkripsi dan terenkripsi.
d. Untuk hasil pengujian serangan pada telepon terenkripsi menggunakan ARP *poisoning* yang menyebabkan SoftPhone MicroSIP yang digunakan oleh *Client* B rusaknya hasil rekaman suara dan kejadian ketika *Client* A melakukan *end call* tetapi *Client* B tidak dapat melakukan *end call* secara otomatis dapat ditindaklanjuti penyebab dari kedua kejadian tersebut pada penelitian selanjutnya.