Analisis Keamanan Enkripsi End-to-end Aplikasi Whatsapp

Stella Ribli 18219027
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
riblistella@gmail.com

***Abstract*—Salah satu bidang teknologi yang berkembang secara pesat adalah bidang komunikasi, salah satunya adalah aplikasi penukaran pesan. Salah satu aplikasi yang terkenal dan sering didengar pada kalangan adalah Whatsapp. Selain perkembangan teknologi meningkat, tingkat kriminalitas dalam pencurian data pada internet juga terus meningkat. Kriptografi merupakan ilmu untuk mencegah hal tersebut. Ilmu kriptografi mempelajari cara membuat data lebih sulit untuk diakses dengan tujuan akhir membuat algoritma paling kompleks sehingga peretas sulit untuk meretas informasi. Salah satu metode kriptografi adalah *vigenere cipher.* Makalah kali ini akan menganalisis tingkat keamanan proses enkripsi *end-to-end* aplikasi Whatsapp.**

Kata Kunci—Whatsapp, Pesan, Kriptografi, Enkripsi, End-to-end

I. Introduction

Pada era digital ini yang terus berkembang ini, internet telah menjadi suatu hal yang penting bagi kehidupan manusia dan semakin sering digunakan secara intensif, bahkan pengguna internet di Indonesia mencapai 76.8% hingga 2020. [1]

Salah satu bidang teknologi yang berkembang secara pesat adalah bidang komunikasi, salah satu contohnya adalah Whatsapp, sebuah aplikasi pengiriman pesan. Pertukaran informasi secara jarak jauh dapat dilakukan dengan mudah, hanya dengan mengetik pesan dan mengirimkannya ke pihak yang bersangkutan.

Seiring peningkatan ilmu manusia terkait teknologi, banyak teknologi yang terus berkembang namun penyalahgunaan ilmu tersebut juga meningkat. Suatu pihak dapat melakukan serangan yang dapat merusak kerahasiaan dari informasi konfidensial. Keberhasilan dalam peretasan suatu sistem dapat berdampak fatal jika berada di tangan pihak yang tidak bertanggungjawab.

Kasus yang ada di era ini seharusnya menjadi peringatan agar kita dapat lebih peduli dengan keamanan informasi yang ada dan melakukan pencegahan awal. Umumnya, banyak informasi pada internet yang bersifat rahasia dan hanya dapat diakses pihak tertentu.

Ilmu kriptografi menjadi solusi yang ada saat ini untuk masalah keamanan informasi. Ilmu kriptografi memiliki tujuan yaitu menjaga keamanan pesan ketika dikirimkan ke suatu pihak. Karena itu, suatu aplikasi pengirim pesan wajib memastikan keamanan dari proses pertukaran informasi.

Whatsapp dalam proses pengiriman pesan antar pihak menggunakan fitur *end-to-end encryption* dengan basis *the signal protocol,* yang didesain oleh Open Whisper Systems.. Fitur ini memungkinkan agar hanya pengirim dan penerima yang dapat mengakses informasi yang ditukar pada aplikasi.

Dengan konsiderasi pentingnya suatu pesan dienkripsi secara optimal pada proses pengiriman pesan, penulis melakukan analisis tingkat keamanan aplikasi pengiriman pesan Whatsapp dalam mengenkripsi pesan yang dikirimkan suatu pihak terhadap pihak lainnya.

II. Metodologi Penelitian

A. Metode Penelitian

Penelitian ini dimulai dengan rasa ingin tahu dari penulis atas topik yang kemudian divalidasi dengan melakukan studi literatur. Data penelitian dicari seeluruhnya dengan studi literatur pada web, jurnal, dan sumber lainnya dengan memanfaatkan internet.

B. Batasan Penulisan

Penelitian pada makalah ini dibatasi dengan bahasan *encryption end-to-end* pada aplikasi Whatsapp, hanya membahas pertukaran pesan yang dilakukan pada aplikasi.

III. Dasar Teori

A. Kriptografi

Kriptografi adalah sebuah ilmu yang telah ada sejak tahun 400 sebelum masehi [7]. Ilmu kriptografi terus berkembang pesat karena dibutuhkannya komunikasi secara rahasia. Kriptografi adalah sebuah kata dari bahasa Yunani, yang berarti *kryptos* dan *graphein.*

Kriptografi secara ilmu dibagi menjadi dua, yaitu kriptografi tradisional dan kriptografi modern. Keduanya

membantu agar suatu pesan dapat dikirimkan secara rahasia dengan berbagai cara.

Algoritma kriptografi secara gambaran umum memiliki tiga fungsi dasar yaitu enkripsi, dekripsi, dan kunci. Enkripsi mengubah plaintext menjadi ciphertext, Dekripsi sebaliknya, dan kunci adalah nilai rahasia yang memungkinkan proses enkripsi dan dekripsi unik.

Kriptografi terfokus untuk memastikan beberapa aspek keamanan seperti *confidentiality, integrity, authentication,* dan *non-repudiation.* Namun, kriptografi tidak dapat seluruhnya menyelesaikan masalah keamanan informasi yang ada karena tidak ada algoritma kriptografi yang sempurna dan pastinya ada celah, atau sering disebut *vulnerability.*

B. Whatsapp

Whatsapp adalah sebuah aplikasi yang didirkan oleh Jan Koum dan Brian Acton pada tahun 2009. Whatsapp merupakan sebuah aplikasi pertukaran pesan antar pihak yang menggunakan aplikasi. Aplikasi Whatsapp mempermudah proses pengiriman pesan. Whatsapp diciptakan dengan tujuan awal yaitu alternatif untuk *Short Message Service (SMS).* Whatsapp memiliki kelebihan yang tidak dimiliki oleh SMS yaitu tidak membutuhkan biaya pulsa untuk setiap pesan yang dikirimkan dan tidak ada batas untuk semua tempat di dunia. Whatsapp saat ini sudah digunakan oleh lebih dari 2 miliar orang dari 180 negara.

Whatsapp memiliki beberapa fitur berupa pengiriman teks, foto, video, berbagi lokasi, dan lain-lain. Whatsapp kini mempunyai beberapa jenis, yaitu [5]:

1. Aplikasi Whatsapp
   Aplikasi Whatsapp berkembang pada sistem operasi iOS maupun Android yang merupakan versi standar yang dikembangkan oleh perusahaan.

2. Whatsapp Web
   Whatsapp web merupakan versi Whatsapp yang dapat dibuka dengan browser komputer atau desktop.

3. Whatsapp Business
   Whatsapp Business merupakan aplikasi Whatsapp yang diperuntukkan bagi bisnis skala besar maupun kecil.

4. Whatsapp MOD
   Whatsapp MOD merupakan aplikasi Whatsapp versi non-resmi dengan beberapa modifikasi fitur.

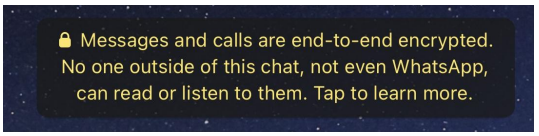
Logo Whatsapp dapat dilihat pada gambar berikut.

Gambar 1. Logo Whatsapp

C. Enkripsi End-to-end

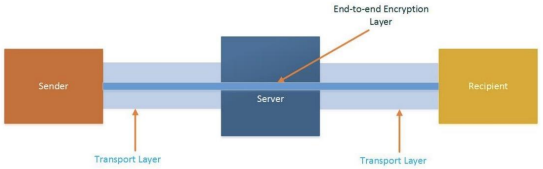
Enkripsi *end-to-end* adalah suatu teknik untuk mengamankan pengiriman informasi dengan cara mengenkripsi konten pada *chat* bentuk apapun. Enkripsi *end-to-end* mengirimkan informasi melalui jaringan yang hanya diketahui oleh pengirim dan penerima.

Fitur enkripsi *end-to-end* Whatsapp akan muncul secara otomatis dan ada pada versi terbaru dari Whatsapp dan dapat dilihat informasinya seperti pada gambar berikut.



Gambar 2. Tampilan Informasi Fitur Enkripsi End-to-end

Gambaran umum enkripsi *end-to-end* dapat dilihat pada gambar berikut.



Gambar 3. Enkripsi End-to-end
(sumber: https://budi.rahardjo.id/files/courses/2016/EL6115-2016-23214353-Report.pdf)

Pada aplikasi Whatsapp, sistem enkripsi end-to-end dilakukand egnan desain basis Open Whisper System.

E. Kunci Publik

Ada beberapa tipe kunci publik yang digunakan pada fitur enkripsi Whatsapp seperti berikut.

- Identity Key Pair
  Identity Key Pair adalah pasangan kunci jangka panjang Curve25519, yang akan dibuat saat instalasi.
- Signed Pre Key
  Signed Pre Key adalah pasangan kunci jangka menengah Curve25519, yang akan dibuat pada tahap instalasi dan akan berubah-ubah pada waktu tertentu.

- One-Time Pre Keys
  One-Time Pre Keys adalah sebuah barisan untuk pasangan kunci kunci Curve25519 yang dibuat pada tahapan instalasi dan hanya akan muncul saat dibutuhkan.

F. Session Key

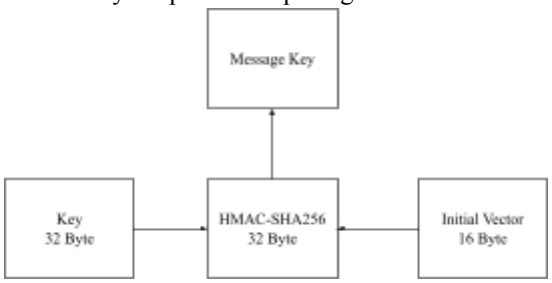
Ada beberapa tipe *session key* dengan waktu terdefinisi yang digunakan pada fitur enkripsi Whatsapp seperti berikut.

- Root Key
  Root Key adalah sebuah nilai dengan panjang 32-byte untuk menciptakan Chain Keys.

- Chain Keys
  Chain Keys merupakan sebuah nilai dengan panjang 32-bye untuk menciptakan Message Keys.

- Message Keys
  Message Keys merupakan sebuah nilai dengan panjang 80 byte dengan spesifikasi 32 byte digunakan untuk kunci AES-256, 32 byte untuk kunci HMAC-SHA256, dan 16 bytes untuk IV.

  Gambarannya dapat dilihat pada gambar berikut.



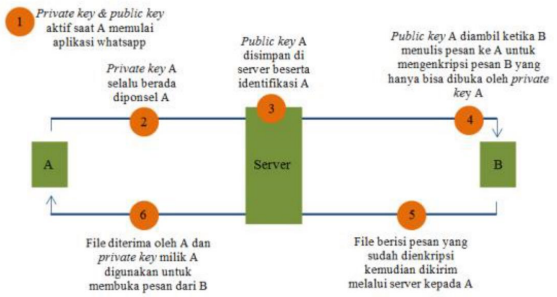
Gambar 3. Gambaran Message Keys

G. Linking Secret Keys

Linking Secret Key merupakan sebuah nilai dengan panjang 32-byte yang dibuat pada *device* yang digunakan untuk memverifikasi HMAC *payload* yang diterima dari suatu *device.* Proses ini dilakukan pada aplikasi Whatsapp dengan melakukan *scanning* sebuah QR Code.

IV. Pembahasan

Proses enkripsi pesan Whatsapp secara umum dapat dilihat pada gambar berikut.



Gambar 4. Gambaran Proses Enkripsi Pesan [8]

Ada beberapa tahapan dalam proses enkripsi *end-to-end* pengiriman pesan aplikasi Whatsapp yang akan dijelaskan untuk beberapa tahapan pentingnya.

A. Client Registration

Tahapan ini merupakan tahapan dimana registrasi pengguna akan dilakukan pada *device* yang digunakan. Proses terbagi menjadi dua, dimana ada proses registrasi untuk *device* yang memilki sifat *device* inti atau *primary device* dan ada *company device registration,* dimana *device* yang digunakan bukanlah *device* inti.

- *Primary Device Registration*
  Pendaftaran awal Whatsapp akan dilakukan dengan cara mentransmisi kunci public Identity Key, Signed Pre Key, dan juga One-Time Pre Keys ke server. Whatsapp akan menyimpan kunci tersebut sesuai dengan pengguna terkait.

- *Companion Device Registration*
  Tahapan ini memiliki syarat yaitu pengguna harus sudah pernah membuat akun utama sebelumnya. Berikut adalah tahapan menghubungkan ke *companion device:*

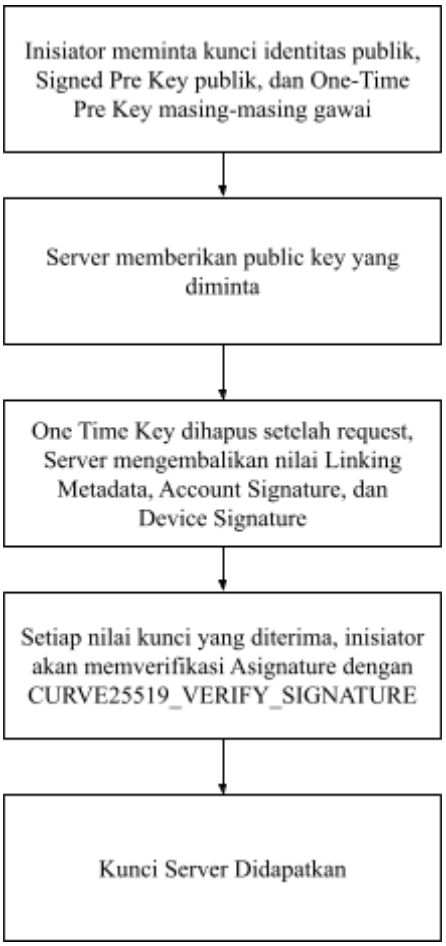
  1. Klien menampilkan kunci publik Identity Key, Linking Secret Key, yang tidak diketahui oleh pihak Whatsapp.
  2. Klien utama scan QR Code dan menyimpan informasi Identity Key
  3. Linking Metadata dibuat dan muncul daftar data bernama ListData
  4. Tanda tangan untuk akun dibuat dengan nama Asignature menggunakan tipe CURVE25519.
  5. List data dibuat lagi, dan bagian inti akan menserialisasikan data terhubung yang mengandung data metadata, Identity Key, dan tanda tangan akun.
  6. Dibuat hubungan antara HMAC, PHMAC, dan HMAC-SHA256
  7. List data, list tanda tangan, dan PHMAC akan dikirimkan ke Whatsapp server

8. Server menyimpan daftar data dan daftar tanda tangan.
9. Linking data dan PHMAC dikirimkan ke *companion device*
10. PHMAC diverifikasi, Ldata diubah menjadi metadata, data primer, dan data tanda tangan.
11. Tanda tangan digital diciptakan dengan CURVE25519
12. *Companion device* melakukan upload terhadap kunci-kunci ke server Whatsapp
13. Server menyimpan data sesuai akun yang terhubung

B. Inisiasi Setup Sesi

Langkah ini adalah langkah dimana pengguna berkomunikasi mulai berkomunikasi dengan pengguna lainnya. Pada tahapan ini, akan terbentuk satu sesi dengan di awal saat melakukan instalasi akan terbentuk sebuah sesi.
WhatsApp menggunakan pendekatan "client-famout" untuk mengirimkan pesan ke beberapa perangkat, dimana hanya dengan satu kali pengiriman pesan akan terenkripsi sesinya berpasangan untuk setiap perangkat dengan akun yang sama.

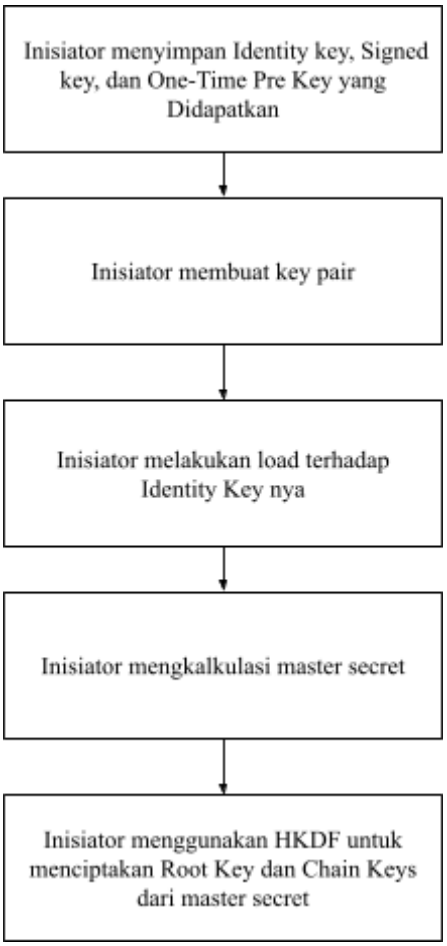
Berikut adalah tahapan dalam menginisiasi suatu sesi yang digambarkan melalui suatu diagram hingga mendapatkan kunci.



Gambar 5. Tahapan Mendapatkan Kunci Server

Proses ini hanya bisa terjadi jika verifikasi seluruhnya berhasil. Jika tidak, inisiator akan menghentikan sesi enkripsi dan tidak akan mengirimkan pesan apapun.

Setelah kunci sudah didapatkan dan verifikasi identitas gawai sudah dilakukan, inisiator akan membuat sesi enkripsi dengan masing-masing gawai dengan tahapan seperti diagram berikut.



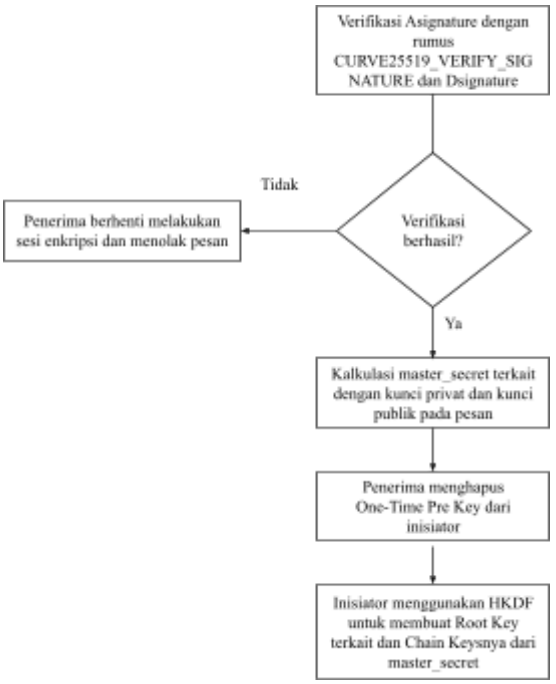
Gambar 6. Tahapan Inisiasi Sesi

Tahapan ini hanya dapat terjadi jika ada One Time Pre Key yang tersedia. Jika tidak ada One Time Pre Key tersedia, ECDH di hapus.

C. Penerimaan Setup Sesi

Setelah ada suatu sesi enkripsi, sistem dapat langsung mengirimkan pesan ke penerima. Hingga penerima merespon, inisiator akan menyediakan informasi bahwa dibutuhkan sebuah sesi *corresponding*.

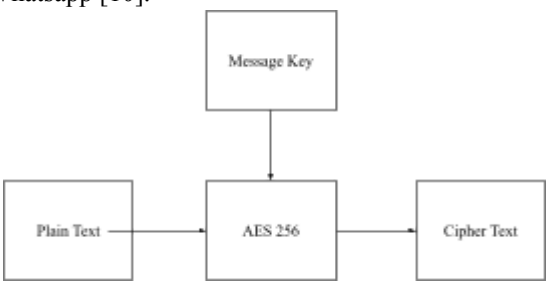
Berikut adalah tahapan saat penerima menerima pesan dengan informasi setup sesi.



Gambar 7. Diagram Penerimaan Setup Sesi

D. Pertukaran Pesan

Berikut adalah blok diagram enkripsi pesan pada Whatsapp [10].



Gambar 8. Blok Diagram Enkripsi Pesan

Proses penukaran pesan dilakukan dengan cara mengkalkulasi message key dari chain key di awal dengan spesifikasi berikut.

1. Message Key = HMAC-SHA256(Chain Key, 0x01)
2. Chain Key = HMAC-SHA256(Chain Key, 0x02)

Setelah itu, chain key dari root key akan dikalkulasi sebagai berikut.

1. ephemeral_secret = ECDH(Ephemeralsender, Ephemeralrecipient)
2. Chain Key, Root Key = HKDF(Root Key, ephemeral_secret)

Chain hanya akan digunakan dari satu user, sehingga message keys tidak akan digunakan secara berulang.

Kesimpulan

Berdasarkan analisis yang telah dilakukan, kami mempelajari beberapa tahapan yang dilakukan pada fitur enkripsi *end-to-end* aplikasi Whatsapp seperti tahapan pada saat pembuatan akun, inisiasi sesi, penerimaan sesi, dan juga pertukaran pesan.

Algoritma yang digunakan juga sangat kompleks sehingga keamanan pengguna sangat terjaga dalam prosesnya. Walaupun begitu, pastinya suatu sistem dapat suatu saat diretas. Namun, berdasarkan analisis yang telah dilakukan, Whatsapp sudah cukup baik dalam menjaga informasi pengguna sehingga Whatsapp memiliki teknik enkripsi yang baik dan terpercaya.

Penghargaan

Penulis mengucapkan syukur sebesar-besarnya kepada Tuhan yang Maha Esa karena masih memberikan kesehatan dan atas berkat-Nya sehingga penulis dapat mengerjakan tugas makalah ini. Penulis juga ingin mengucapkan terima kasih atas dukungan teman dan keluarga pada setiap proses pembelajaran

Penulis ingin mengucapkan syukur juga kepada Bapak Dr. Ir. Rinaldi Munir, M.T. atas bantuannya dan ilmunya yang telah dibagikan pada mata kuliah II4031 Kriptografi dan Koding, yang telah berjasa banyak dalam pengembangan ilmu selama satu semester.

Referensi

Berikut adalah referensi yang digunakan untuk proses pengerejaan penelitian ini.

[1] Santria, Ummi, and Nira Arsoetar. "Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp."

[2] Permana, Angga Aditya. "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android." Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi 4.3 (2018): 110-115.

[3] https://www.sekawanmedia.co.id/blog/pengertian-kriptografi/

[4] https://www.whatsapp.com/about/?lang=id

[5] https://dianisa.com/pengertian-whatsapp/

[6] D. J. Bernstein, “Curve25519: New Diffie-Hellman speed records,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2006, vol. 3958 LNCS, pp. 207-228

[7] Santria, Ummi, and Nira Arsoetar. "Penggunaan Enkripsi End-to-End dalam Pengamanan Pesan dan Video Call pada Whatsapp."

[8] Jamaluddin, Jamaluddin, Roni Jhonson Simamora, and Karyawati Sitepu. "Konsep Pengamanan Pesan dengan Teknik Enkripsi End to End pada WhatsApp Messenger." (2016).

[9] Urva, Gellysa. "Analisis Penggunaan Enkripsi End To End Pada Aplikasi Whatsapp Messengger." Jurnal Unitek 10.1 (2017): 34-45.

[10] https://budi.rahardjo.id/files/courses/2016/EL6115-2016-23214353-Report.pdf

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, 25 Mei 2021

Stella Ribli
18219027