Pencegahan Replay Attack Menggunakan MAC dan Timestamp dalam Pengiriman Pesan

Adi Hendro 18218009
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
adi.h.maill[at]gmail.com

***Abstract*—Pada era modern komunikasi antara dua pihak dilakukan melalui berbagai media elektronik seperti internet dengan mudah. Internet menawarkan manfaat seperti cepat, memiliki jangkauan luas, dan berbiaya rendah. Namun, terdapat masalah keamanan yang mengancam pengiriman pesan di internet. Pihak ketiga dapat menyadap isi pesan tanpa sepengetahuan pengirim dan penerima, hingga berpura-pura menjadi salah satu pihak dan menyalahgunakan pesan yang dikirimkan. Teknik penyerangan yang disebut replay attack memungkinkan pihak ketiga mengulangi data transimisi sebelumya untuk memperoleh hak akses. Pesan dapat dilindungi dari replay attack melalui penambahan timestamp dan dipastikan integritasnya menggunakan MAC.**

Keywords—hash; MAC; replay attack; sequence number; timestamp

I. Introduction

Jarak dan waktu tidak lagi menjadi halangan saat berkomunikasi di era modern ini. Dua orang yang berada di belahan bumi berbeda dapat berkirim pesan secara instan melalui internet. Biaya yang dikeluarkan juga sangat kecil dibandingkan komunikasi tradisional melalui surat. Siapa pun dapat dengan mudah mengirim pesan tanpa perlu ilmu pengetahuan mendalam, cukup memiliki akses internet dan perangkat pintar.

Namun, segala kemudahan yang diberikan internet tidak membuatnya kebal dari serangan orang tidak bertanggung jawab. Pesan yang dikirim melalui internet dapat diakses dan disalahgunakan tanpa sepengetahuan kedua pihak. Permasalahan ini dapat menyebabkan kerugian baik secara finansial maupun moral bagi pengguna internet.

Berbagai mitigasi telah diterapkan sejak awal pemakaian internet. Enkripsi dapat melindungi pesan dari pihak ketiga dan memastikan hanya pengirim dan penerima asli saja yang dapat membaca pesan. Pengirim pesan akan melakukan enkripsi menggunakan kunci simetri yang ditentukan sebelumnya, lalu mengirimkan pesan terenkripsi ke tujuan. Penerima pesan akan menerima pesan terenkripsi dan membukanya menggunakan kunci simetri tadi. Pihak ketiga yang menyadap pesan terenkripsi tidak memiliki kunci sehingga tidak dapat melihat isi pesan.

Menggunakan enkripsi dengan protokol modern terbukti ampuh mencegah bocornya informasi. Tapi pihak ketiga masih dapat menyalahgunakan pesan terenkripsi dengan mengubah bit di dalamnya. Pihak penerima akan menganggap pesan tersebut asli berasal dari penerima walaupun telah diubah. Akibatnya terjadi modifikasi informasi di tengah jalan. Pihak ketiga juga dapat menyimpan pesan terenkripsi tadi untuk digunakan di lain waktu seperti berpura-pura menjadi pengirim sehingga mendapat hak akses yang tidak seharusnya. Teknik pengulangan kembali pesan disebut dengan replay attack.

Pencegahan terhadap modifikasi pesan dapat dilakukan dengan tambahan hash satu arah dari pesan. Hash dibuat menggunakan kunci rahasia yang hanya dimiliki pengirim dan penerima. Hash seperti ini disebut dengan MAC (message authentication code). Dengan demikian pihak ketiga tidak dapat membuat hash palsu.

Selain itu pencegahan terhadap pengulangan pesan atau replay attack dilakukan dengan menambahkan timestamp pada setiap pesan. Timestamp digabungkan dengan pesan dan dihitung dengan MAC. Dengan demikian pesan yang sama tidak dapat diulang di waktu yang berbeda.

II. Basic Theory

A. Fungsi Hash

Fungsi hash merupakan suatu fungsi yang melakukan identifikasi pesan dengan panjang sembarang menjadi suatu string dengan panjang tetap.

Fungsi hash menjadi identitas atau fingerprint dari pesan semula. Perubahan sekecil apapun pada pesan asli akan menghasilkan hash yang berbeda total. Dengan demikian jika hasil hash tidak berubah, maka dapat dipastikan bahwa pesan asli juga tidak berubah. Hash akan menjaga integritas pesan dalam pengiriman.

Secara sederhana fungsi hash dapat ditulis sebagai:

$$h = H(M)$$

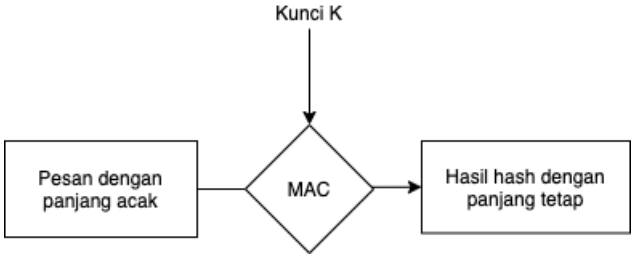
dengan h sebagai hasil hash, H sebagai fungsi hash, dan M sebagai pesan.

Selain itu hash juga memiliki ciri-ciri tidak dapat dikembalikan menjadi pesan semula (one-way function) dan sangat sulit untuk menemukan dua pesan berbeda yang dapat menghasilkan hash yang sama (collision resistance).

B. Message Authentication Code

Message Authentication Code atau disingkat MAC adalah fungsi hash satu arah yang digunakan untuk mengidentifikasi suatu pesan. Sama seperti fungsi hash, perubahan sekecil apapun pada pesan akan menghasilkan hash yang sangat berbeda. MAC juga memiliki sifat one-way function dan sifat collision resistance.

Perbedaan MAC dibandingkan fungsi hash biasa adalah perlunya kunci rahasia untuk membangkitkan nilai MAC. Tanpa kunci rahasia tidak mungkin dapat menghasilkan MAC yang sesuai. Berbeda dengan fungsi hash lain yang dapat dihasilkan secara bebas tanpa ada kunci. Sehingga jika hasil MAC suatu pesan valid, dapat dipastikan MAC tersebut dibuat oleh pengirim pesan asli dan bukan oleh pihak ketiga (diasumsikan kunci rahasia tidak bocor).

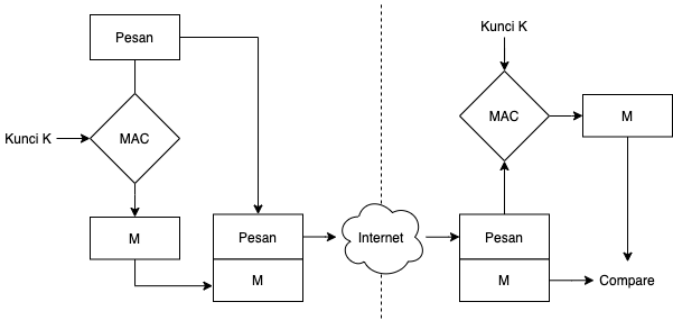


Secara sederhana fungsi hash dapat ditulis sebagai:

$$M' = MAC_k(M)$$

dengan M' sebagai hasil hash, MAC sebagai algoritma MAC, k sebagai kunci rahasia, dan M sebagai pesan.

Penggunaan MAC dalam memastikan integritas pesan digambarkan pada diagram di bawah. Pengirim menghitung MAC dari pesan yang akan dikirimkan menggunakan kunci K. Kunci K ini rahasia serta diketahui oleh pengirim dan penerima. Hasil MAC berupa M akan ditempelkan pada pesan lalu dikirim melalui internet. Penerima memisahkan pesan dengan M dan menghitung MAC dari pesan tersebut. Hasil perhitungan MAC akan dibandingkan dengan M yang dikirimkan. Jika kedua M sama maka pesan dipastikan tidak dimodifikasi.

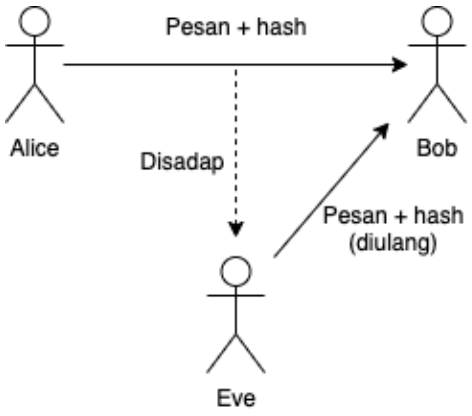


Penerapan integritas pesan di atas tidak melakukan enkripsi pada pesan. Pihak ketiga di internet dapat melihat isi pesan yang dikirim. Maka untuk melindunginya pesan dapat dienkripsi menggunakan kunci rahasia lain. Enkripsi dapat dilakukan setelah MAC dihitung dan digabungkan dengan pesan. Penerima akan melakukan dekripsi dahulu setelah menerima pesan. Tipe ini disebut internal error code. Akan tetapi jika ada perubahan pesan saat pengiriman, penerima malah melakukan dekripsi secara sia-sia. Masalah ini diatasi dengan tipe external error code, yaitu melakukan enkripsi pesan di awal sebelum MAC dihitung. Maka integritas pesan dapat langsung dicek setelah diterima. Tipe ini akan menghemat waktu dengan tidak melakukan dekripsi saat pesan diubah.

C. Replay Attack

Replay attack adalah teknik penyerangan dengan mengulang pengiriman data transmisi valid kepada target. Pihak ketiga menyadap pesan terenkripsi yang dikirim melalui jaringan dan menyimpannya untuk digunakan kemudian. Lalu pihak ketiga mengirim pesan tadi lagi kepada target dan berpura-pura menjadi sumber yang asli. Perlu diperhatikan bahwa pesan yang disadap asli dan mengandung MAC yang asli pula. Target yang melihat keaslian pesan akan tertipu dan menganggap pihak ketiga sebagai pengirim yang benar.

Ancaman keamanan yang dihasilkan oleh replay attack dapat berupa pemberian akses token kepada penyadap. Digambarkan pada ilustrasi di bawah terdapat komunikasi antara Alice dan Bob. Alice ingin memasuki suatu website yang dikelola Bob dengan mengirimkan password dan hashnya. Bob menerima permintaan Alice dana memberi izin masuk. Tanpa diketahui Alice dan Bob, Eve menyadap komunikasi mereka. Eve mencatat password beserta hash yang dikirimkan Alice. Eve tidak dapat memperoleh kembali passwordnya karena sudah dilakukan fungsi hash satu arah. Akan tetapi Eve dapat mengirimkan data tadi kepada Bob beberapa saat kemudian untuk meminta akses. Bob melihat password dan hash dari Eve benar, lalu menyetujui akses masuk Eve.



Perlindungan terhadap replay attack adalah sebagai berikut:

1. Memberi session ID untuk setiap sesi

   Setiap komunikasi harus disertai dengan session ID yang sesuai. Bob akan menghitung session ID dari one time token yang dibangkitkan. Alice menerima session

ID ini dan menggunakannya saat mengirim pesan ke Bob. Setelah sesi selesai session ID tersebut dianggap tidak berlaku lagi oleh kedua pihak. Penyadap pun tidak dapat memakai data sebelumnya di sesi baru.

2. Menambahkan timestamp

   Setiap pesan yang dikirim diberikan timestamp yang tersinkronisasi antara pengirim dan penerima. Alice yang ingin mengirim pesan akan menambahkan tanggal dan waktu saat itu ke dalam pesan, lalu menghitung MAC dan mengirimkan ke Bob. Bob yang menerimanya akan melihat hasil perhitungan MAC yang disesuaikan dengan waktu penerimaan. Jika perbedaan waktu masih dalam toleransi yang diterima, maka pesan tersebut dianggap asli berasal dari Alice.

3. Membuat one-time password

   Setiap pesan yang dikirim akan diberikan one-time password. Password ini hanya digunakan sekali, bukan dalam satu sesi seperti session ID. Dengan demikian Alice dan Bob dapat berkomunikasi dengan pasti. Namun pembuatan one-time password dan pembagiannya antara Alice dan Bob cukup sulit dilakukan setiap saat.

III. Implementasi Program

Solusi yang diimplementasi dalam pencegahan replay attack adalah penghitungan MAC dari pesan yang ditambahkan dengan timestamp saat pengiriman. Program dibuat dalam bahasa python. Library yang digunakan untuk membangkitkan MAC adalah hmac. Library ini memiliki method new yang menerima parameter kunci, pesan, dan jenis hash yang digunakan.

1. Pertama dilakukan pembangkitan MAC

```
digest = hmac.new(bytearray(kunci, 'utf-8'), bytearray(pesan, 'utf-8'), hashlib.sha1)
```

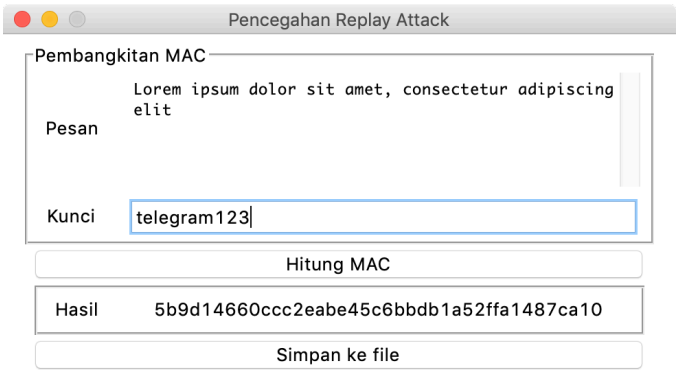
2. Lalu diambil timestamp dari tanggal, jam, menit, dan detik saat pembangkitan

```
ct = datetime.datetime.now(datetime.timezone.utc)
```

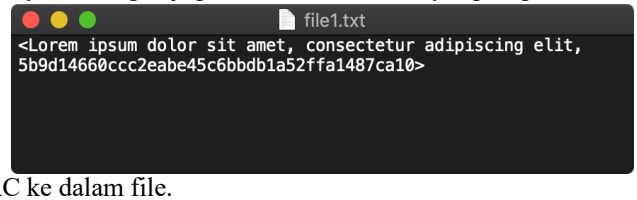
3. Kemudian timestamp tersebut akan ditambahkan ke dalam pesan dan MAC dihitung kembali.

```
digest.update(bytearray(ct.strftime('%Y/%m/%d-%H:%M:%S'), 'utf-8'))
hasil_mac= digest.hexdigest()
self.state['hasil'].set(hasil_mac)
```

Berikut adalah tampilan antarmuka program dalam python. Pengguna memasukkan pesan dan kunci. Lalu menekan



tombol hitung MAC. MAC akan dihitung dan berganti setiap detiknya. Terdapat juga tombol untuk menyimpan pesan dan



MAC ke dalam file.

References

[1] Malladi, Sreekanth, Alves-Foss, Jim, and Heckendorn, Robert B. 2002. "On Preventing Replay Attacks on Security Protocols"

[2] Munir, Rinaldi. 2021. Slide Kuliah II4031 Kriptografi dan Koding: Fungsi Hash

[3] Munir, Rinaldi. 2021. Slide Kuliah II4031 Kriptografi dan Koding: MAC (Message Authentication Code)

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

Adi Hendro 18218009