Analisis Serangan Pihak Ketiga pada Protokol Kesepakatan Kunci Diffie-Hellman

Banu Wirawan Yohanes

Program Studi Sistem Komputer,
Fakultas Teknik Elektronika dan Komputer,
Universitas Kristen Satya Wacana, Salatiga
banu.yohanes@staff.uksw.edu

Ringkasan

Penemuan protokol kesepakatan kunci Diffie-Hellman merupakan salah satu tonggak penting perkembangan kriptografi dengan menggunakan algoritma kunci publik. Namun implementasi protokol Diffie-Hellman sering mengalami kelemahan pada keamanan data yang cukup mengganggu. Terkadang serangannya tampak begitu halus dan tidak terdeteksi oleh perancang protokol. Pada artikel ini dibahas tentang sebuah serangan dari pihak ketiga dalam komunikasi menggunakan protokol Diffie-Hellman secara teori dan implementasi programnya. Dari analisis hasilnya diharapkan para praktisi keamanan data pada sistem dan jaringan komputer memperoleh informasi untuk merancang dan membangun versi/varian protokol Diffie-Hellman yang lebih aman dan efisien.

Kata kunci: protokol Diffie-Hellman, serangan pihak ketiga (*man in the middle attack*)

1. Pendahuluan

Pada era informasi digital ini semakin marak transaksi yang dilakukan lewat web. Pada awalnya berkembangnya jaringan komputer dan web tidak dirancang menyertakan fitur keamanan. Namun, seiring dengan pertumbuhan web yang pesat maka dikembangkan metode untuk mengamankan transaksi pada internet. Salah satu metode adalah dengan menggunakan protokol keamanan.

Protokol keamanan merupakan algoritma atau mekanisme komunikasi antara dua pihak atau lebih untuk mencapai tujuan keamanan tertentu. Misalnya, protokol otentikasi dan permulaan kunci yang memperbolehkan dua pihak atau lebih berkomunikasi melalui jaringan yang tidak aman untuk memeriksa identitas satu sama lain dan memulai sebuah kunci rahasia yang seragam.

Salah satu skema pertukaran/kesepakatan kunci yang masih digunakan dan diturunkan secara luas sampai kini adalah protokol Diffie-Hellman (untuk selanjutnya ditulis DH) [1]. Meskipun tampak sederhana, protokol DH memiliki persoalan yang hampir tidak kentara. Kerentanan tersebut ditambah dengan kurang tepatnya pemahaman akan masalah keamanan data. Kedua hal tersebut yang menyebabkan sering dijumpainya implementasi protokol kriptografi yang kurang memadai. Artikel ini membahas salah satu serangan pada protokol DH dengan menunjukkan prosesnya secara matematis.

Penulisan artikel ini diawali dengan latar belakang persoalan pada bagian 1. Bagian 2 menyajikan dasar teori matematis yang diperlukan untuk memahami protokol DH.

Bagian 3 menampilkan beberapa jenis serangan yang mungkin pada protokol DH, dan salah satu contoh serangan dari pihak ketiga di antara pihak-pihak yang berkomunikasi. Simulasi serangan ini dibuat menggunakan program PARI/GP [2] dan hasil analisisnya dibahas pada bagian 4. Akhirnya bagian 5 berisi kesimpulan.

2. Protokol Kesepakatan Kunci Diffie-Hellman

Protokol DH digunakan untuk memberikan kunci rahasia bersama antar dua pihak, sebutlah Alice (A) dan Bob (B), melalui saluran komunikasi publik. Seorang penyerang yang mendengarkan secara diam-diam pesan yang dikirim oleh Alice dan Bob tidak dapat mengetahui kunci rahasia bersama yang dipakai. Hal ini merupakan primitif yang bermanfaat karena rahasia bersama dapat diturunkan menjadi kunci sesi rahasia yang dapat digunakan pada sistem kriptografi simetris, seperti *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES), atau *Message Authentication Codes* (MAC). Alasan penggunaan kunci sesi adalah untuk membatasi jumlah *ciphertext* yang tersedia dari sebuah kunci tunggal, membatasi efek, baik waktu dan jumlah data, dari sebuah kunci yang terungkap atau terkompromi, dan membuat independensi antar sesi.

2.1. Dasar Teori

Perhitungan pada protokol DH dikerjakan pada sebuah grup.

Grup Sebuah grup $(G,\bigstar)$ terdiri dari sebuah himpunan G dan suatu operasi biner $\bigstar$ pada elemen-elemen dari G. Operasi $\bigstar$memiliki sifat berikut:

1. Asosiatif: $a \bigstar (b \bigstar c) = (a \bigstar b) \bigstar c$, untuk semua $a, b, c \in G$.
2. Identitas: Ada sebuah elemen $1 \in G$, disebut identitas, yang memenuhi $1 \bigstar a = a \bigstar 1 = a$, untuk setiap $a \in G$.
3. Invers: Untuk setiap $a \in G$, ada sebuah nilai yang dinyatakan dengan sedemikian hingga $a \bigstar a^{-1} = a^{-1} \bigstar a = 1$.

Sebuah grup Abelian merupakan suatu grup yang memiliki sifat tambahan berikut:

4. Kumutatif: $a \bigstar b = b \bigstar a$, untuk semua $a, b \in G$.

Untuk grup terbatas (G *finite*), orde dari sebuah grup dinyatakan sebagai ukuran (kardinalitas) dari G. Orde dari sebuah elemen a pada grup terbatas G dinyatakan sebagai nilai t terkecil sehingga $a^t = \underbrace{a \bigstar a \bigstar .. \bigstar a}_{t} = 1$.

Grup Siklik Sebuah grup siklik merupakan sebuah grup dengan sifat bahwa terdapat sebuah elemen g sedemikian hingga seluruh elemen pada G dapat dinyatakan sebagai g^i untuk setiap nilai i yang berbeda. Jika g menghasilkan seluruh elemen pada grup $(G,\bigstar)$, maka g adalah generator dan dikatakan menghasilkan $(G,\bigstar)$. Orde dari sebuah generator g sama dengan orde grup yang dihasilkannya.

Subgrup G' merupakan subgrup dari G jika $(G',\bigstar)$ membentuk sebuah grup dan ($G' \subseteq G$). Jika G adalah grup terbatas, maka orde dari subgrup G' akan selalu membagi orde dari G, berdasarkan teori Lagrange [3].

Contoh grup yang sering dipakai pada protokol DH adalah himpunan $\mathbf{Z}p^*$ dengan perkalian modulus p dimana p merupakan bilangan prima, grup pengali dari field $\mathbf{F}2^m$ dan grup penjumlah dibentuk oleh koleksi titik yang dinyatakan oleh sebuah kurva elips dari sebuah field terbatas. Seluruh grup ini memiliki sifat bahwa eksponensiasi menggunakan komputasi yang murah dan bahwa menghitung log diskrit tampak sulit,

atau secara komputasi tidak mudah. Pada artikel ini, grup merupakan himpunan = {1, 2, ..., p-1} dengan perkalian modulus p (p prima) dan seluruh operasi akan dikerjakan pada grup. Misalnya g^y berarti g^y mod p.

2.2. Cara kerja Protokol Diffie-Helman

Pada awalnya, Alice (A) dan Bob (B) sepakat menggunakan sebuah bilangan prima yang besar p dan elemen g ($2 \leqslant g \leqslant p$-2) yang menghasilkan sebuah subgrup siklik orde tinggi. Umumnya nilai-nilai tersebut telah ditetapkan sebelum sistem dibuat dan digunakan untuk banyak protokol, untuk menghindari kemungkinan dimana nilai-nilai tersebut telah menjadi parameter publik yang digunakan oleh setiap orang. Kemudian protokol berjalan dengan tahapan kerja sebagai berikut:

1. A memilih sebuah bilangan x secara acak dari himpunan {1, ..., p-2}. B memilih y secara acak dari himpunan yang sama.
2. A mengirimkan g^x mod p kepada B dan B mengirimkan g^y mod p kepada A.
3. Kunci rahasia bersama adalah $K = g^{xy}$ mod p. A mengetahui x dan g^y, dapat menghitung $(g^y)^x = g^{xy}$ mod p dengan mudah. B dapat menentukan kunci rahasia dengan cara serupa untuk menghitung $(g^x)^y$ mod p.

x dan y merupakan kunci privat, g^x dan g^y merupakan kunci publik, dan g^{xy} merupakan kunci rahasia bersama pada protokol DH. Ketika kunci rahasia hanya dipakai sekali maka disebut kesepakatan kunci rahasia DH *ephemeral*. Asumsi bahwa penyerang yang mendengarkan kanal komunikasi secara diam-diam memiliki akses ke nilai publik tidak dapat menghitung kunci rahasia bersama, disebut asumsi DH. Asumsi DH terkait dengan asumsi log diskrit yang menyatakan bahwa sebuah generator g dari $\mathbf{Z}p^*$ dan sebuah elemen β dari $\mathbf{Z}p^*$, tidak mudah untuk menghitung x di mana g^x ekuivalen dengan β in $\mathbf{Z}p^*$. Berdasarkan fakta bahwa jika log diskrit dapat dihitung secara efisien, maka g^{xy} dapat dihitung dari diketahui g, g^x, dan g^y. Kemudian membatalkan asumsi DH, tetapi penghitungan log diskrit merupakan persoalan yang sulit untuk diselesaikan.

3. Serangan pada Protokol Diffie-Hellman

Secara umum, terdapat tiga kategori jenis serangan terhadap protokol DH:

1. Serangan penolakan layanan (*denial of service*, DoS): Seorang penyerang berusaha untuk memberhentikan Alice dan Bob dari menjalankan protokol. Misalnya, dengan menghapus pesan yang terkirim antara Alice dan Bob atau membanjiri kanal komunikasi dengan proses komputasi/komunikasi yang tidak diperlukan.
2. Serangan dari pihak luar: Seorang penyerang berusaha menganggu jalannya protokol dengan menambahkan, menghilangkan, atau mengulangi pesan-pesan yang dikirimkan. Tujuannya adalah untuk memperoleh pengetahuan berupa informasi yang tidak dapat diperoleh dengan mengamati parameter publik saja.
3. Serangan dari pihak dalam: Salah satu partisipan protokol DH mungkin membuat protokol yang rusak sengaja dijalankan dengan tujuan untuk memperoleh pengetahuan tentang kunci rahasia dari pasangan dalam berkomunikasi. Hal ini penting jika salah satu partisipan memegang kunci rahasia statis yang digunakan pada banyak protokol kesepakatan kunci.

Kemungkinan berhasilnya serangan-serangan tersebut tergantung kepada asumsi tentang pihak penyerang. Misalnya, jika penyerang dapat menghapus dan mengganti

setiap pesan dari saluran komunikasi publik maka serangan penolakan layanan tidak dapat dihindari. Berikut merupakan salah satu jenis serangan dari pihak luar (ketiga) yang memiliki kemampuan untuk mengintersepsi pesan yang dikirim oleh kedua pihak yang sedang berkomunikasi untuk berbagi kunci rahasia bersama menggunakan protokol DH.

3.1. Serangan pihak ketiga (*man in the middle Attack*)

Seorang penyerang yang aktif, Charlie (*C*), mampu menghapus dan menambah pesan dengan mudah mematahkan protokol DH. Dengan mengintersepsi g^x dan g^y dan menggantinya dengan $g^{x'}$ dan $g^{y'}$, Charlie dapat mengelabui Alice dan Bob yang berpikir bertukar kunci rahasia yang sama. Jadi, Alice akan mengira kunci rahasianya adalah $g^{xy'}$ dan Bob akan mengira kuncinya $g^{x'y}$. Serangan dari pihak ketiga yang berada di antara kedua pihak yang sedang berkomunikasi ini disebut serangan *man in the middle atttack* [4], skemanya ditunjukkan oleh Gambar 1.

Alice		**Charlie**		**Bob**
x, g^x	->	x', y', $g^{x'}$	->	y, g^y
	g^x		$g^{x'}$	
$g^{xy'}$	<-	$g^{x'y} = g^{xy'}$	<-	$g^{x'y}$
	$g^{y'}$		g^y	

1.	A -> C:	g^x
2.	C -> B:	$g^{x'}$
3.	B -> C:	g^y
4.	C -> A:	$g^{y'}$

Kunci kesepakatan yang digunakan menjadi K′ = $g^{x'y} = g^{xy'} \bmod p$

Gambar 1. Skema intersepsi pihak ketiga, Charlie, di antara komunikasi Alice dan Bob

Sebuah contoh kasus, Alice dan Bob menggunakan kunci rahasia bersama yang diperoleh dari suatu protokol DH untuk enkripsi simetrik. Misalkan Alice mengirim pesan *m* kepada Bob dan $ENC_K(m)$ menyatakan enkripsi simetri, seperti DES, dari *m* menggunakan kunci rahasia *K*.

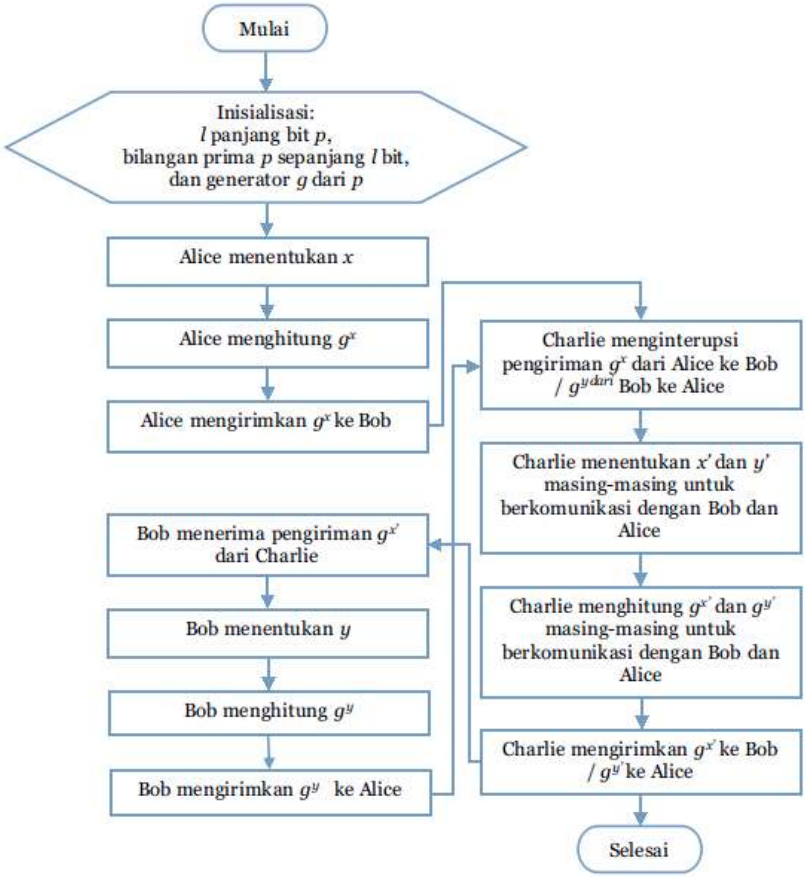
1. *A* mengirim $ENC_{g^{xy'}}(m)$.
2. *C* mengintersepsi $ENC_{g^{xy'}}(m)$ dan men-dekripnya karena tahu $g^{xy'}$.
3. *C* mengganti pesan ini dengan $ENC_{g^{x'y}}(m')$ yang dikirimkan kepada *B*. *m*′ dapat ditetapkan sebagai pesan apapun.

Skema enkripsi ini terkompromi karena privasi dari pesan dilanggar. Meskipun serangan ini sepenuhnya mematahkan protokol DH, tetapi membutuhkan syarat Charlie handal. Dalam kategori serangan cryptanalitik ini diasumsikan Charlie memiliki kemampuan untuk memilih *plaintext* (*chosen plaintext attack*). Charlie dapat mengirimkan sejumlah tak terbatas pesan *plaintext* pilihannya dan memeriksa hasil dari skema kriptografi DH. Misalnya, jika kunci rahasia yang digunakan berdasarkan MAC, maka Charlie perlu mengintersepsi dan memodifikasi setiap pesan terotentikasi untuk mencegah Alice dan Bob mengetahui bahwa kunci mereka tidak identik.

4. Simulasi dan analisis serangan pihak ketiga (*man in the middle attack*) menggunakan PARI/GP

Untuk menunjukkan proses serangan dari pihak ketiga yang berada di antara pihak-pihak yang berkomunikasi digunakan Pari/GP. Pari/GP merupakan sebuah sistem aljabar pada komputer, digunakan terutama untuk implementasi teori bilangan. Selain itu, juga digunakan pada bidang lain dari topologi, analisis numerik, atau fisika.

Pada tahap inisialisasi parameter protokol DH, nilai p sepanjang l bytes dan sebuah generator g, berupa elemen primitif, dihasilkan oleh GP menggunakan fungsi `genP(l)`,. Untuk menetapkan nilai p dan g yang akan dipakai pada sebuah sesi protokol DH, digunakan fungsi `setP(p)` dan `setGen(g)`. Alice dan Bob masing-masing menetapkan kunci privat dan menghasilkan kunci publik menggunakan fungsi `setKeyA(prvKeyA)` dan `setKeyB(prvKeyB)`. Charlie, seorang penyerang di antara Alice dan Bob, menggunakan fungsi `setKeyCA(prvKeyCA)` dan `setKeyCB(prvKeyCB)` untuk menetapkan kunci privat dan menghasilkan kunci publik bagi tiap sesi dimana Charlie berpura-pura sebagai Alice dan Bob. Kemudian, untuk mencari kunci rahasia bersama antara Alice dan Bob menggunakan kunci rahasia Bob dipakai fungsi `sharedKeyBA(prvKeyB)`. Diagram alir interupsi Charlie terhadap pengiriman pesan antara Alice dan Bob ditunjukkan pada Gambar 2.



Gambar 2. Diagram alir serangan pihak ketiga, Charlie, terhadap komunikasi antara Alice dan Bob

```
Man-in-the-middle Attack on Diffie-Hellman Key Exchange
by Banu Yohanes

Enter:
- setP(P)         : to set the prime number P
- setGen(g)       : to set the primitive element (generator) g
- setKeyA(key)    : to set the private key & generate the public key of A
- setKeyCB(key)   : to set the private key & generate the public key of C who impersonate as A to communicate with B
- setKeyB(key)    : to set the private key & generate the public key of B
- setKeyCA(key)   : to set the private key & generate the public key of C who impersonate as B to communicate with A
- sharedKeyBA(key): to find the BA-shared key using B's private key in the original DH protocol
- sharedKeyAC(key): to find the AC-shared key using A's private key
- sharedKeyBC(key): to find the BC-shared key using B's private key

Automatic Generation:
- genP(l)         : to generate P with size l bits
? genP(4)
P = 23
g = 5
? setGen(5)
%15 = 5
? setKeyA(3)
5^3%23 = 10
A sending message (10) --> C who I(B)
? setKeyCB(4)
5^4%23 = 4
C who I(A) sending message (4) --> B
? setKeyB(5)
4^5%23 = 12
B sending message (12) --> C who I(A)
? setKeyCA(6)
1^6%23 = 3
C who I(B) sending message (3) to A
? sharedKeyBA(5)
19
? sharedKeyAC(3)
4
? sharedKeyBC(5)
12_
```

Gambar 3. Simulasi serangan pihak ketiga pada protokol DH menggunakan PARI/GP

Dari hasil simulasi menggunakan program PARI/GP di Gambar 3 tampak bahwa protokol DH dapat dipatahkan oleh serangan *man in the middle* yang sederhana. Untuk mengatasi persoalan tersebut perlu ditambahkan metode otentikasi yang menjamin keabsahan pihak-pihak yang berkomunikasi dan pesan-pesan yang dikirimkan.

5. Kesimpulan

Metode otentikasi untuk menghindari serangan pihak ketiga (*man in the middle attack*) dapat dilakukan dengan mengecek keabsahan tanda tangan digital atau sebuah MAC secara sederhana menggunakan fungsi verifikasi atau keabsahan pesan yang lebih rumit. Keabsahan pesan harus menjamin beberapa hal termasuk pesan tidak dimodifikasi, pesan dikirim oleh pihak pengirim kepada tujuan tertentu, pesan tidak dikirim ulang, dan pesan dikirimkan pada rentang waktu tertentu.

Berdasarkan analisis pada protokol DH, terdapat beberapa rekomendasi yang dapat dipakai sebagai acuan untuk membuat implementasi protokol kesepakatan kunci DH. Pertama, temukan pengiriman pesan yang tidak lazim dengan memastikan bahwa g^x, g^y, dan g^{xy} tidak boleh sama dengan 1, pastikan bahwa g^x dan g^y lebih besar dari 1 dan kurang dari p-1, dan pilih x dan y dari himpunan {2, ..., p-2} [5].

Kedua, pertimbangan orde generator g. Dekomposisi faktor prima pada orde g seharusnya tidak semuanya berisi bilangan prima yang kecil. Subgrup yang dihasilkan oleh g seharusnya tidak memiliki orde yang rendah. Jika memungkinkan, buat dan gunakan sebuah generator yang memiliki orde bilangan prima yang besar.

Ketiga, pilihlah parameter yang aman. Serangan yang mengekspoitasi parameter yang berbeda dari sistem seharusnya memakan jumlah waktu yang setara. Pada protokol DH, parameter yang harus diseimbangkan adalah nilai dari p, jangkauan eksponen dan ukuran dari kunci yang diturunkan dari kunci rahasia bersama DH. Untuk tingkat

keamanan yang memadai sampai tahun 2025 disarankan untuk menggunakan p sepanjang 2174 bit, jangkauan eksponen 158 bit dan panjang kunci turunan 89 [6].

Daftar Pustaka

[1] W. Diffie, M. Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory 22*, h. 644 – 654, 1976.

[2] The Pari Group, "*A Tutorial for Pari/GP (version 2.7.0)*," Institut de Mathématiques de Bordeaux, France, 2014.

[3] T.W. Hungerford, *Algebra*, Holt, Rinehart dan Winston, New York, 1974.

[4] R.L. Rivest, A. Shamir, "How to expose an eavesdropper," *Communications of the Association for Computing Machinery*, vol. 27, no. 4, h. 393-395, 1984.

[5] E. Rescorla, "*Diffie-Hellman Key Agreement Method*," Request for Comments: 2631 Network Working Group, RTFM Inc., 1999. [Online], `https://www.ietf.org/rfc/rfc2631.txt`, diakses 10 Maret 2015.

[6] A.K. Lenstra, D.E.R. Verheul, Selecting cryptographic key sizes, versi pendeknya muncul di Proceedings of the Public Key Cryptography Conference (PKC2000) dan Autumn'99 PricewaterhouseCoopers CCE newsletter, 1999.