Sistem Pengamanan Data Pemilihan Umum e-Voting dengan Menggunakan Algoritma SHA-1

Abdurrosyid Broto Handoyo and 13510107[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510107@stei.itb.ac.id

***Abstrak*—Penggunaan teknologi komputer dalam proses pemilihan umum dikenal dengan istilah e-voting. Namun, dalam pelaksanaan e-voting, masalah keamanan menjadi pusat perhatian. Untuk membuat sistem e-voting menjadi lebih aman, maka teknik kriptografi pun digunakan. Pada makalah ini akan dibahas bagaimana penggunaan fungsi hash kriptografi untuk menjamin keamanan data pada sistem e-voting. Penggunaan fungsi hash kriptografi membuat sistem yang dibuat menjadi lebih simple karena tidak ada proses enkripsi dan dekripsi sepertimana kriptografi kunci privat ataupun kunci publik. Hasil fungsi hash kriptografi didesain untuk tidak reversible sehingga cocok dengan kriteria keamanan sistem pemilu. Fungsi hash kriptografi yang dibahas di sini adalah SHA-1 karena masih terjamin kekebalannya terhadap serangan-serangan secara kriptografi oleh kriptanalis.**

***Kata Kunci*—Pemilihan umum, e-voting, fungsi hash kriptografi, SHA-1**

I. PENDAHULUAN

Pemilu merupakan sebuah pesta rakyat yang sudah lumrah terjadi di masyarakat Indonesia. Hampir seluruh pemilihan jabatan pemimpin saat ini melalui proses pemilihan umum, baik dalam skala yang besar ataupun dalam skala yang lebih kecil. Walaupun demikian, masih banyak proses pemilihan umum yang masih belum sepenuhnya menerapkan prinsip dasar pemilu, yaitu luber (langsung, umum, bebas dan rahasia). Terutama pada prinsip langsung, bebas dan rahasia dari data pemilu tersebut.

Saat ini pemilu biasanya berlangsung menggunakan 2 cara, yaitu pemilihan dengan kertas dan pemilihan melalui e-vote. Pemilihan umum melalui kertas adalah yang paling sering digunakan saat ini, namun terkadang pemilihan dengan cara ini dinilai cukup merepotkan. Kemudian berkembanglah e-vote pada pemilu dengan skala tertentu. Biasanya pada skala organisasi, pemilu diadakan menggunakan e-vote agar lebih mudah.

Dengan berkembangnya e-vote maka sisi keamanan akan menjadi acuan utama. Dengan media digital, serangan manipulasi data akan lebih sering terjadi. Pada beberapa kejadian e-vote yang ditemukan, aspek keamanan data tidak sepenuhnya dijaga dengan baik. Manipulasi data masih dapat dilakukan hanya dengan mengubah pilihan orang lain dan memilihkan orang yang tidak memilih dalam pemilu. Bila data dapat secara mudah dimanipulasi, maka integritas pemilu akan sangat dipertanyakan.apalagi dalam prinsip langsung, umum, bebas dan rahasia.

Bagaimana kita dapat menjamin pemilu secara e-vote berjalan secara langsung, bebas dan rahasia? Salah satu cara yang dapat kita gunakan adalah menggunakan kriptografi untuk mengamankan data sehingga pemilu yang langsung, bebas dan rahasia tersebut dapat terlaksana dengan baik.

II. DASAR TEORI

2.1. Pemilihan Umum

Di dalam Negara yang menerapkan sistem pemerintahan demokrasi, pemilihan umum adalah hal yang sangat lazim terjadi. Hal ini merupakan salah satu implementasi dari sistem demokrasi. Dalam sistem ini, rakyat dapat secara langsung memilih pemimpinnya sendiri.

Pemilihan umum merupakan proses pemilihan orang-orang untuk mengisi suatu jabatan politik tertentu. Jabatan-jabatan tersebut beraneka-ragam, mulai dari presiden, wakil rakyat di berbagai tingkat pemerintahan, sampai kepala desa. Pada konteks yang lebih luas, pemilu dapat juga berarti proses mengisi jabatan-jabatan seperti ketua organisasi ataupun pemimpin dalam bentuk apapun.

Beberapa prinsip dasar pemilihan umum yang harus dipenuhi adalah langsung, umum, bebas dan rahasia. Langsung berarti pemilih harus memberikan suaranya secara langsung dan tidak boleh diwakilkan. Umum berarti pemilihan umum dapat diikuti seluruh warga negara yang sudah memiliki hak menggunakan suara. Bebas berarti pemilih diharuskan memberikan suaranya tanpa ada paksaan dari pihak manapun, kemudian Rahasia berarti suara yang diberikan oleh pemilih bersifat rahasia hanya diketahui oleh si pemilih itu sendiri.

2.2. E-vote

Seiring dengan perkembangan zaman, telah banyak penelitan mengenai pemanfaatan media elektronik untuk

mendukung proses pemungutan suara menggantikan pengumungutan suara secara manual. Pemanfaatan media lektronik inilah yang disebut e-voting (electronic voting). E-voting secara definisi adalah proses pemungutan suara yang memanfaatkan elektronik. Penelitian ini telah berlangsung sejak tahun 1869 ketika Thomas A. Edison menerima paten dari Amerika Serikat untuk sebuah "electronic vote recorder" yang rencananya akan digunakan pada Kongres. Namun, teknologi tersebut masih belum digunakan hingga sekrang dalam skala nasional di Amerika karena masih belum siap dalam menggunakan sistem ini.

Penelitian terkait e-voting masih terus dilakukan sampai sekarang. Ada bermacam-macam teknologi yang digunakan dalam mengembangkan e-voting tersebut. Berikut ini beberapa persyaratan yang harus dipenuhi dalam suatu sistem e-voting

1. Accuracy (akurasi) yaitu ketepatan hasil perhitungan suara. Ketepatan ini meliputi tidak ada satupun pihak yang diperbolehkan mengubah suara yang telah masuk, semua suara yang valid dihitung dengan tepat, dan suara yang tidak valid tidak boleh dihitung.
2. Democracy (demokrasi) yaitu hanya calon pemilih yang memenuhi syarat berhak untuk memilih dan setiap pemilih hanya berhak untuk memasukkan suaranya satu kali.
3. Privacy (privasi) yaitu tidak seorang pun yang dapat menghubungkan seseorang dengan hasil pilihannya.
4. Robustness yaitu tidak ada gangguan yang menghalangi pelaksanaan pemungutan suara. Jadi aspek ini berkaitan erat dengan aspek security (keamanan).
5. Verifiability yaitu setiap orang dapat membuktikan bahwa tidak ada manipulasi terhadap hasil perhitungan.
6. Uncoercibility yaitu tidak adanya paksaan kepada pemilih dalam menentukan pilihannya. Agar tidak terjadi maka pemilih harus tidak dapat membuktikan hasil pilihannya kepada orang lain (receipt freeness).
7. Fairness yaitu setiap orang tidak dapat mengetahui hasil pemilihan sebelum proses pemilihan selesai dan dilakukan perhitungan suara.
8. Verifiable participation yaitu mampu membuktikan apakah seseorang telah melakukan pemungutan suara atau belum.

2.3. Kriptografi

Kriptografi merupakan sebuah ilmu yang mempelajari penjagaan keamanan dari sebuah data atau pesan yang kita miliki. Ilmu kriptografi sudah berkembang sejak masa Julius Caesar untuk mengamankan pesan dalam sebuah peperangan. Keamanan pesan sangat penting dalam berbagai hal, karena banyak informasi yang secara kebijakan tidak untuk beritahukan kepada publik.

Dalam proses pengamanan pesan menggunakan kriptografi, terdapat beberapa komponen penting yang menjadi inti dari keamanan sebuah pesan, yaitu:

- Data Confidentiality

Aspek kerahasiaan pesan yang dimiliki. Dalam kriptografi, hal ini menjadi fokus utamanya. Kriptografi mencoba untuk menjaga dan melindungi kerahasiaan pesan sehingga pesan tersebut tidak dapat diketahui oleh semua orang. Selain itu, dalam aspek ini juga harus memperhitungkan kemudahan bagi orang yang memang diperbolehkan membuka pesan tersebut.

- Authentication

Aspek ini berkaitan dengan autentifikasi siapa pengirim pesan tersebut. Salah satu permasalahan keamanan adalah bisa saja kita mendapatkan pesan dari orang ketiga yang seolah-olah menjadi orang yang ingin mengirim pesan kepada kita. Pesan palsu ini sangat berbahaya karena dapat merusak komunikasi yang terjalin antara dua pihak yang ingin berkomunikasi. Hal ini telah menjadi salah satu *concern* utama dalam keamanan informasi.

- Data Integrity

Aspek ini berkaitan mengenai bagaimana keabsahan pesan yang dikirim. Bisa saja ketika pesan tersebut dikirim, di tengah jalan ada orang yang mengintercept kemudian mengubah isi pesan tersebut sehingga pesan gagal disampaikan dengan baik. Oleh karena itu, kriptografi harus memberikan layanan penjamin keaslian pesan yang dikirimkan dengan berbagai cara, antara lain bila teks cipher telah diubah, maka pesan sudah tidak dapat lagi dibuka. Hal ini dapat mengindikasikan terdapat interceptor yang mengubah isi pesan tersebut.

- Nonrepudiation

Aspek ini adalah bagaimana mencegah entitas yang berkomunikasi menyangkal bahwa pesan tersebut tidak dikirim oleh mereka. Aspek ini membahas juga bagaimana kita dapat membuktikan pesan tersebut benar-benar dikirim oleh orang yang mengklaim tersebut. Bila hal ini tidak diperhatikan,maka bisa saja dalam sebuah transasksi pembelian, orang yang membeli mengklaim bahwa transaksi itu bukan darinya meskipun sebenarnya dia yang melakukan pembelian.

Cara untuk pengamanan pesan telah berkembang dari masa ke masa. Secara umum terdapat 3 cara pengamanan pesan dengan kriptografi yang popular saat ini, yaitu enkripsi kunci simetri, enkripsi kunci publik dan fungsi hash . Masing-masing memiliki kelebihan dan kekurangan masing-masing, sehingga masing-masing cara digunakan untuk kebutuhan yang berbeda-beda.

2.4. Fungi Hash Kriptografi

Fungsi hash kriptografi adalah sebuah fungsi hash yang memetakan data kepada sebuah string sebagai representasi bit dengan panjang tertentu yang telah ditentukan. Fungsi hash didesain agar pengubahan sedikit saja pada data akan mengubah hasil hash secara signifikan.

Sebuah fungsi hash kriptografi yang ideal harus memenuhi 4 kriteria berikut ini, yaitu:

- Hash value mudah dihitung bile diberikan input pesan seperti apapun
- Tidak feasible untuk mencari message bila diberikan sebuah hash value
- Tidak feasible untuk memodifikasi pesan tanpa mengubah hash value
- Tidak feasible untuk mencari 2 pesan yang memiliki hash value yang sama

Saat ini fungsi hash kriptografi banyak digunakan untuk keamanan informasi pada digital signature, message authentication codes (MACs). Selain itu dapat digunakan untuk verifikasi integritas pesan, verifikasi file dan generator angka pseudorandom.

2.5. Secure Hash Algorithm 1

SHA-1 adalah sebuah fungsi hash kriptografi yang didesain National Security Agency (NSA) dari Amerika Serikat pada tahun 1993. Saat ini SHA sudah memiliki 4 versi yaitu SHA-0, SHA-1, SHA-2 dan SHA-3. SHA-1 adalah fungsi SHA yang paling sering digunakan untuk keamanan aplikasi dan protokol seperti SSL, SSH, TLS dan S/MIME. Selain untuk keamanan, SHA-1 juga digunakan untuk menjamin integritas data pada aplikasi-aplikasi seperti Git.

SHA-1 akan menghasilkan 160 bit *message digest* dengan prinsip yang mirip dengan MD4 dan MD5. Secara umum, skema dari pembuatan SHA-1 dapat dirumuskan dalam framework seperti berikut:

1. Penambahan bit-bit pengganjal (padding bit)
2. Penambahan panjang pesan pada 64 bit terakhir agar total panjang pesan menjadi kelipatan 512 bit
3. Pesan dipecah menjadi masing-masing 16 buat 32 bit
4. Siapkan buffer inisialisasi sepanjang 160 bit
   - H_0 = 0x67452301
   - H_1 = 0xEFCDAB89
   - H_2 = 0x98BADCFE
   - H_3 = 0x10325476
   - H_4 = 0xC3D2E1F0
5. Blok pesan sebesar 16 buah 32 bit diexpand menjadi 80 buah 32 bit dengan persamaan berikut:

$$W_i = (W_{i-16} \oplus W_{i-14} \oplus W_{i-8} \oplus W_{i-3}) \lll 1$$

untuk

$$16 \leq i \leq 79$$

6. Lakukan state update dengan persamaan sebagai berikut

$$A_{i+1} = (A_i \ll 5) + f(B_i, C_i, D_i) + E_i + K_i + W_i$$

$$B_{i+1} = A_i$$

$$C_{i+1} = B_i \ll 2$$

$$D_{i+1} = C_i$$

$$E_{i+1} = D_i$$

Dengan fungsi f sebagai berikut

- $f_i(B,C,D)$
  `(B AND C) OR ((NOT B) AND D)`
  → `[0 <= i <= 19]`
- $f_i(B,C,D)$
  `B XOR C XOR D`
  → `[20 <= i <= 39]`
- $f_i(B,C,D)$
  `(B AND C)OR(B AND D)OR(C AND D)`
  → `[40 <= i <=59]`
- $f_i(B,C,D)$
  `B XOR C XOR D`
  → `[60 <= i <= 79]`

Dan konstanta K_i sebagai berikut

- $K_i = 0x5A827999$
  → `[0 <= t <= 19]`
- $K_i = 0x6ED9EBA1$
  → `[20 <= t <= 39]`
- $K_i = 0x8F1BBCDC$
  → `[40 <= t <= 59]`
- $K_i = 0xCA62C1D6$
  → `[60 <= t <= 79]`

dan inisialisasi sebagai berikut

$$A_0 = H_0,\ B_0 = H_1,\ C_0 = H_2,\ D_0 = H_3,\ E_0 = H_4$$

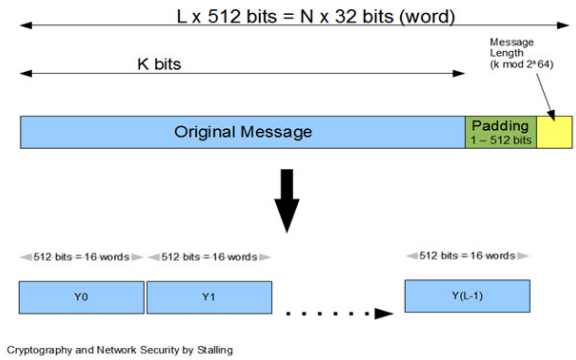
Setelah perulangan tersebut berakhir pada $i = 79$, maka dilakukan perubahan kepada buffer sebagai berikut:

$$H_0 = A_{79}, \quad H_1 = B_{79}, \quad H_2 = B_{79}, \quad H_3 = B_{79}, \quad H_4 = B_{79}$$

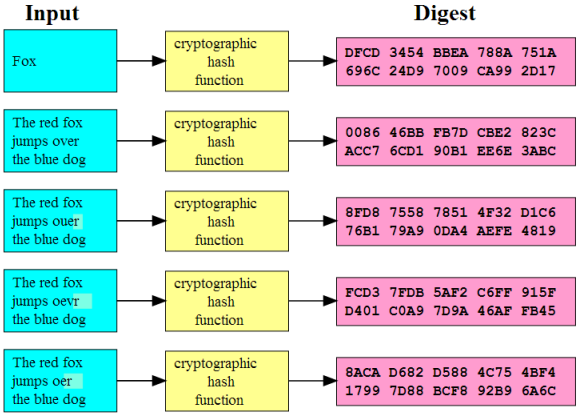
7. Langkah nomor 5-6 dilakukan terus menerus pada setiap blok pesan yang dipecah sesuai langkah nomor 3.
8. Hasil akhir dari fungsi hash ini adalah bila kita menggabungkan H_0, H_1, H_2, H_3 dan H_4 secara big-endian. Dinyatakan sebagai berikut:

   `Hash = H0 append H1 append H2 append H3 append H4`

Gambar-1 menunjukkan visualisasi dari framework kerja fungsi hash SHA-1



Gambar-2 menunjukkan contoh hasil hash SHA-1 dan keacakan hash value yang ditimbulkan. Dari gambar tersebut dapat kita lihat bahwa pengubahan sedikit saja dari input dapat menyebabkan hash value berubah secara drastis.



Hingga saat ini SHA-1 masih dianggap cukup aman dari segi keamanan algoritma. SHA-1 masih merupakan algoritma paling populer meskipun SHA-3 sudah dirilis. Walaupun masih dianggap aman tetapi SHA-1 sudah terbukti dapat diserang dengan *Collision Attack* secara optimal dengan kompleksitas teoritik 2^{51} pemanggilan fungsi hash menggunakan disturbance vector. Namun demikian, masih belum ditemukan sebuah algoritma yang mangkus untuk menjebol SHA-1 dengan serangan *Preimage Attack*, yaitu serangan pada fungsi hash untuk menentukan pesan yang mungkin dari sebuah hash value.

2.6. Serangan pada Fungsi Hash Kriptografi SHA-1

Untuk menentukan level keamanan dari sebuah algoritma fungsi hash kriptografi, maka harus dibuktikan kekebalannya terhadap serangan-serangan yang sudah umum digunakan. Berikut ini adalah daftar serangan pada fungsi hash kriptografi secara umum, yaitu:

- Collision Attack
  Serangan jenis ini mencoba mencari dua buah input yang dapat menghasilkan hash value yang sama. Dalam hal ini, diketahui sebuah input dan hash value yang berkaitan. Collision attack ini terbagi menjadi dua tipe, yaitu:
  - Standard collision attack
    Mencari dua pesan berbeda $m1$ dan $m2$ sehingga $hash(m1) = hash(m2)$
  - Chosen-prefix collision attack
    Diberikan dua prefix yang berbeda p1 dan p2, carilah m1 dan m2 sehingga $hash(p1 \,//\, m1) = hash(p2 \,//\, m2)$ dengan // adalah fungsi konkatenasi

Collision attack ini sangat berbahaya dalam proses digital signature. Misalkan Alice ingin menipu Bob, bila algoritma hash tersebut vulnerable terhadap serangan ini, maka skenario seeprti berikut dapat terjadi:

1) Alice membuat dua buah dokumen, yaitu m yang merupakan dokumen asli dan m' yang merupakan dokumen palsu yang telah dimodifikasi.
2) Alice mencari posisi-posisi yang dapat diubah pada dokumen m sedemikian sehingga pengubahan tersebut tidak mengubah makna dari dokumen m. Seperti contoh, penambahan koma, penambahan baris kosong, mengubah sinonim, jumlah spasi pada sebuah kalimat, dsb. Dengan cara ini Alice mendapatkan versi dokumen m yang sangat banyak.
3) Alice mencari posisi-posisi yang dapat diubah pada dokumen palsu m' sedemikian sehingga pengubahan tersebut tidak mengubah makna dari dokumen m. Seperti contoh, penambahan koma, penambahan baris kosong, mengubah sinonim, jumlah spasi pada sebuah kalimat, dsb. Dengan cara ini Alice mendapatkan versi dokumen palsu m' yang sangat banyak.
4) Kemudian ia mengulangi cara 2 dan 3 terus hingga menemui kondisi hash(m)=hash(m')
5) Alice mengirim dokumen m kepada Bob untuk ditandatangani. Kemudian bob, memberikan digital signaturenya pada dokumen tersebut.
6) Alice mengopi digital signature dari dokumen m pada dokumen palsu m'.
7) Alice sekarang memiliki sebuah dokumen palsu m' yang dapat dibuktikan ditandatangani oleh Bob.

- Preimage Attack
  Preimage attack adalah serangan pada fungsi hash kriptografi untuk mencari pesan dari sebuah hash value yang spesifik. Sebuah algoritma fungsi hash kriptografi masih dianggap memiliki keamanan yang tinggi bila belum dapat ditembus oleh serangan ini.

  Kekebalan algoritma fungsi hash kriptografi dapat dikategorikan menjadi dua bentauk, yaitu:

  - Kekebalan preimage
    Untuk seluruh output, pencarian input untuk mendapatkan output yang ditentukan tidak feasible secara komputasi. Dengan kata lain bila kita mengetahui y sebagai hasi dari $hash(x) = y$,

maka mencari x tidak feasible secara komputasi untuk seluruh harga y.

- Kekebalan second-preimage
  Pencarian sebuah input lain yang menghasilkan output yang sama dengan sebuah input, misalkan x tidak feasible secara komputasi. Dengan kata lain, bila diketahui x, maka second-preimage adalah sebuah x' sedemikian sehingga $hash(x) = hash(x')$.

- Birthday Attack
  Birthday attack adalah sebuah serangan kriptografi yang memanfaatkan properti dari *birthday problem* pada teori probabilitas. Serangan ini bergantung pada lebih tingginya kemungkinan collision pada serangan random yang patternnya seperti *birthday problem*. Secara umum, birthday attack adalah bagaimana melakukan collision attack memanfaatkan properti dari birthday problem. Selain untuk menyerang algoritma fungi hash kriptografi, birthday attack juga dapat digunakan untuk menyerang system Domain Name Server (Dell-SecureWorks, 2007)

- Bruteforce Attack
  Bruteforce attack merupakan sebuah serangan yang dapat diaplikasikan pada seluruh algoritma kriptografi. Pada dasarnya serangan ini mencoba seluruh kemungkinan solusi dari sebuah permasalahan yang diberikan. Namun, komplektias dari bruteforce attack untuk algoritma fungsi hash kriptografi yang baik membutuhkan waktu yang sangat lama dan tidak feasible secara teoritis maupun praktis.

- Rainbow Table Attack
  Rainbow table attack merupakan sebuah tabel pre-komputasi yang biasanya digunakan untuk menyerang hash dari password. *Rainbow table* ini biasanya menyimpan pasangan nilai dan hash value dari kata-kata yang cukup umum digunakan. Bila password kita pada suatu situs menggunakan kata-kata yang umum, kemudian seseorang mengambil hash value password kita dari database server, maka ia dapat mendeduksi password kita dari *rainbow table* ini.

Hingga saat ini algoritma fungsi hash kriptografi SHA-1 masih kebal terhadap mayoritas serangan-serangan yang disebutka di atas. Dengan kata lain, masih belum ditemukan cara yang mangkus untuk mengeksploitasi SHA-1. Namun, SHA-1 telah beberapa kali diteliti mengenai kekebalannya pada collision attack. Salah satu algoritma paling mangkus yang telah ditemukan saat ini adalah menggunakan disturbance vector dengan kompleksitas teoritis 2^{51} kali pemanggilan fungsi hash. Walaupun demikian, pada implementasinya di e-voting kali ini collision attack tidak berpengaruh pada keamanan sistem yang akan dijelaskan pada makalah ini.

III. KRITERIA PESAN SISTEM E-VOTE

Pada sebuah proses pemilihan umum, seorang pemilih akan memilih salah seorang calon dari daftar calon yang telah ditentukan. Proses pemilihan ini dapat dirumuskan pada beberapa tahap sebagai berikut:

- Pemilih mendatangi tempat pemilihan yang ditentukan
  Tempat pemilihan ini dapat berbagai macam bentuknya. Dalam hal e-vote maka tempat pemilihan adalah aplikasi voting yang dapat diakses oleh pemilih

- Verifikasi identitas pemilih
  Pemilih harus memberikan bukti mengenai identitas dirinya agar dipenuhi kriteria berikut:
  - Pemilih adalah orang yang terdaftar pada daftar pemilih yang ditentukan
  - Orang yang datang memilih adalah benar pemilih yang terdaftar
  - Pemilih tersebut belum melakukan voting sebelumnya

- Pemilih memilih calon yang diinginkan
  Proses ini harus dilakukan secara rahasia, sehingga tidak ada orang lain yang dapat mengakses data pemilihan dari pemilih. Selain itu, pemilih seharusnya tidak dalam tekanan pihak lain untuk memilih seorang calon pada fase ini.

- Data pemilihan dikirimkan pada tempat penyimpanan
  Proses ini harus menjamin integritas data yang dikirim. Data tersebut tidak boleh berubah, bila terjadi sebuah serangan pada data pemilihan maka harus terdeteksi oleh sistem di dalamnya.

- Pemilih selesai melakukan proses pemilihan

Setelah waktu yang ditentukan untuk pemilihan umum berakhir, maka dilakukan penghitungan suara terhadap hasil pemilu. Penghitungan suara ini akan menentukan siapa yang memenangi pemilu kali ini. Bila panitia pemilu telah menetapkan secara resmi pemenang dari pemilu, maka mekansime selanjutnya akan diserahkan kepada instansi terkait.

Berdasarkan framework rangkaian kegiatan pemilu di atas, kita dapat merumuskan beberapa kriteria sistem keamanan pesan dan data yang harus dipenuhi yaitu:

- Pesan yang dikirimkan harus memiliki informasi mengenai
  - Identitas pemilih
  - Pilihan yang dipilih oleh pemilih

- Pesan yang dikirimkan tidak bisa dimodifikasi dengan sebuah algoritma yang mangkus

- Hanya pemilh yang dapat memberikan sebuah pesan pemilhan yang valid

- Sistem harus dapat mendeteksi bila terjadi serangan pada pesan pemilihan yang dikirim

- Sistem harus dapat mendeteksi bila terjadi kasus di

mana seorang pemilih memilih lebih dari satu kali (hanya pilihan pertamanya saja yang akan dihitung, pilihan yang dikirimkan selanjutnya akan diabaikan oleh sistem)

- Bila terdapat orang di luar daftar pemilih melakukan pemilihan, maka dapat terdeteksi oleh sistem keamanan e-vote ini
- Pemilih dapat melakukan verifikasi pilihan yang dimasukkan olehnya, untuk menjamin keabsahan pemilu yang berlangsung.

IV. STRUKTUR PESAN E-VOTE

Pada sistem pesan yang dirumuskan kali ini harus memenuhi syarat dan kriteria yang telah disebutkan sebelumnya. Desain pesan yang akan diamankan harus meliputi otentifikasi dari pemilih dan dari sistem. Hal ini ditujukan agar dapat dijamin keabsahan dari pesan yang dikirim.

Pesan yang dikirimkan dan disimpan pada basis data sistem dibuat sama persis karena kita menggunakan fungsi hash kriptografi sehingga tidak perlu proses enkripsi dan dekripsi. Selain itu, hal ini dikarenakan kemungkinan serangan saat pesan dikirimkan dan serangan saat pesan disimpan dalam basis data. Sehingga ketika penyimpanan pada basis data, masih disimpan dalam bentuk hash value.

Berdasarkan karakteristik sistem e-voting pada bab sebelumnya, maka pesan yang didesain ini memiliki format sebagai berikut

$$[nomor\ identitas]\_[password\ user\ dari\ sistem]\_$$

$$[pilihan\ calon]\_[kode\ pemilu]\_[salt]$$

Berikut ini adalah penjelasan detail mengenai setiap atribut yang dipilih pada pesan tersebut:

- Nomor Identitas
  Nomor identitas dari pemilih yang telah disepakati oleh panitia penyelenggara pemilihan umum. Nomor identitas ini berasal dari sebuah identitas yang dimiliki oleh semua pemilih yang terdaftar. Misalkan dalam pemilu organisasi kemahasiswaan, maka digunakan NIM sebagai nomor identitas.

- Password user dari sistem
  Sistem akan memberikan sebuah password kepada pemilih melalui sebuah media privat milik pemilih. Media privat ini haruslah sebuah media yang tidak akan dishare antar pemilih. Dalam sistem ini, media email dipilih karena cukup memenuhi syarat tersebut. Sedangkan password yang diberikan sistem adalah hasil fungsi hash dari password yang degenerate oleh sistem.

- Pilihan calon
  Pada bagian ini, dituliskan pilihan dari pemilih. Pilihan ini akan berbentuk angka dengan format %2d (format string pada bahasa C). Bila pemilih memilih calon 1, maka akan tertulis 01. Panitia pemilu lah yang akan menentukan urutan dari calon-calon terdaftar.

- Kode pemilu
  Setiap event pemilu yang diadakan oleh sistem ini, akan memiliki sebuah kode khusus. Hal ini digunakan agar tidak dimungkinkannya terjadi sebuah user memberikan vote pada pilihan calon 1 di dua sistem pemilu yang berbeda namun hasil hash yang didapat sama persis, bila terjadi kesamaan password dari sistem yang terjadi pada 2 pemilu berbeda.

- Salt
  Salt ini merupakan data random yang dimiliki aplikasi untuk menambah ketahanan aplikasi terhadap serangan secara pada fugsi hash kriptografi, terutama secara Rainbow Table. Operasi bruteforce untuk mendapatkan sebuah hash value yang valid pun akan semakin sulit. Data random

Contoh pesan data pemilihan adalah sebagai berikut:

Pesan pemilihan pada calon 1:
```
13510107_666bebb906e822c728dd9080a0755
128abe6e4ee_01_dbccc9f10f8a8cfcd121a67
651ad2038d00ec2a3_&%@1sbx*$
```

Pesan pemilihan pada calon 2:
```
13510107_666bebb906e822c728dd9080a0755
128abe6e4ee_02_dbccc9f10f8a8cfcd121a67
651ad2038d00ec2a3_&%@1sbx*$
```

Password user dari sistem ini merupakan hasil pemetaan SHA-1 dari sebuah nilai tertentu

Bila nilai tersebut kita masukkan pada fungsi hash SHA-1, maka akan menjadi seperti berikut:

Hash value pesan pemilihan pada calon 1:
```
e943e3321aab75ceaf7ee5aa3b2a22bc277506
3b
```

Hash value pesan pemilihan pada calon 2:
```
918f5c742f6a132be9afa8863355717a968e63
59
```

Dari contoh tersebut, pengubahan pilihan dari calon 1 ke calon 1 dapat membuat nilai hash yang sama sekali berbeda dan tidak ada kaitannya sama sekali. Hal ini juga disebabkan oleh aspek diffusion dan confusion dari algoritma fungsi hash kriptografi SHA-1 sangat baik.

Pesan yang dikirimkan melalui jaringan internet adalah [*nomor identitas*]_[*hash value pesan pemilihan*]. Hal ini digunakan oleh sistem untuk melakukan verifikasi dan deteksi pada serangan pada sistem.

V. Sistem Pengiriman dan Penghitungan E-voting

Pesan yang telah dikirimkan melalui jaringan internet ini akan diterima oleh server sistem. Server ini akan melakukan aksi berdasarkan pesan yang dikirimkan oleh user. Server juga harus dapat mendeteksi dan mengantisipasi bila terdapat serangan terhadap sistem e-voting ini.

Server akan mengekstrak hash value dari pesan yang dikirimkan. Hash value inilah yang akan dikirimkan dan disimpan pada basis data server. Dengan penyimpanan pada format demikian, sangat sulit bagi siapapun untuk melakukan modifikasi hasil fungsi hash. Kemungkinan sebuah pengubahan sebuah hash value akan menghasilkan hash value lain yang bermakna adalah sangat kecil.

Selain hal tersebut, basis data penyimpanan data pemilih dan data hash value pesan pemilu dapat berbeda. Hasil hash dari seluruh data hash value pesan pemilau dapat dipublish untuk menjamin data yang disimpan tidak dirusak oleh orang lain. Karena bila data diubah sedikit saja, maka hasil hash dari data pemilu tersebut akan berubah secara signifikan. Hal ini biasa digunakan dalam hal akuntabilitas sistem.

Selain pendefinisian data yang dikirimkan, kita perlu mendefinisikan apa yang harus dilakukan sistem apabila mendapat hash value pesan pemilu. Pada dasarnya sistem akan menyimpan data tersebut dalam basis data hash value, namun dengan alasan keamanan maka prosesnya menjadi sedikit lebih rumit, yaitu sebagai berikut:

a) Pesan pemilihan datang kepada server dari sistem

b) Dengan data identitas yang diberikan, maka server akan mencoba membuat semua kemungkinan hash value yang dibuat oleh user tersebut dengan kombinasi calon yang ada.
   i. Bila data seluruh kemungkinan data belum ada pada basis data hash value, maka masukkan data pada basis data hash value.
   ii. Bila terdapat 1 data hash value sudah ditemukan di dalam sistem, maka sistem memberikan notifikasi pada pihak yang berwenang dalam hal ini dan sistem menolak data pemilihan yang baru ini. Hal ini disebabkan terdapat kemungkinan modifikasi oleh orang yang tidak bertanggung jawab.
   iii. Bila data yang akan dimasukkan tidak terdapat pada seluruh kemungkinan, maka sistem memberikan notifikasi pada pihak yang berwenang dalam hal ini dan sistem menolak data pemilhan yang baru ini. Hal ini disebabkan terdapat kemungkinan serangan pemilihan oleh orang yang tidak bertanggung jawab

Setelah data pemilihan disimpan, maka sistem harus dapat membaca data tersebut. Misalkan kita memiliki dua basis data yang tidak berkaitan, data mengenai pemilih (identitas, password yang diberikan system, kemungkinan pilihan) dan data pesan pilihan yang berisi hash value. Cara penghitungan suara pada sistem ini adalah sebagai berikut:

a) Sort data pesan hash value
   Hal ini bertujuan untuk mempercepat performa penghitungan suara oleh sistem

b) Untuk setiap data pemilih yang melakukan pemilihan, lakukan konstruksi pesan pemilihan untuk setiap calon
   Misalkan untuk calon 1, 2 dan 3:
   `13510107_666bebb906e822c728dd9080a0`
   `755128abe6e4ee_01_dbccc9f10f8a8cfcd`
   `121a67651ad2038d00ec2a3_&%@1sbx*$`
   `13510107_666bebb906e822c728dd9080a0`
   `755128abe6e4ee_02_dbccc9f10f8a8cfcd`
   `121a67651ad2038d00ec2a3_&%@1sbx*$`
   `13510107_666bebb906e822c728dd9080a0`
   `755128abe6e4ee_03_dbccc9f10f8a8cfcd`
   `121a67651ad2038d00ec2a3_&%@1sbx*$`

c) Kemudian pesan tersebut kita hash dengan SHA-1
   Misalkan untuk calon 1, 2 dan 3:
   `e943e3321aab75ceaf7ee5aa3b2a22bc277`
   `5063b`
   `918f5c742f6a132be9afa8863355717a968`
   `e6359`
   `fa4dd352ed8c4236c0bd62278bfb07d2a5b`
   `01f0a`

d) Hasil hash tersebut inilah yang akan kita cek keberadaannya pada basis data sistem. Salah satu dari seluruh kemungkinan tersebut harus muncul pada data hash value dan hanya boleh ada satu kesamaan saja. Bila kesamaan adalah pada calon 3, maka calon 3 mendapatkan 1 suara.

e) Setelah langkah b, c dan d dilakukan maka seluruh data hash value harus sudah terhitung semuanya.

VII. Kesimpulan

Sistem Pengamanan Data Pemilihan Umum e-voting dapat menjadi sebuah alternatif sistem pemilihan umum yang diterapkan selama ini dengan harga yang relatif lebih murah. Sistem ini pun memenuhi kriteria-kriteria umum dari sistem e-voting yang dapat dihandalkan. Namun, tingkat keamanan dari sistem ini sangat bergntung pada kebalnya SHA-1 terhadap serangan-serangan secara algoritma kriptografi.

VIII. UCAPAN TERIMA KASIH

Makalah ini dibuat untuk memenuhi tugas pengganti Ujian Akhir Semester dari mata kuliah IF3058-Kriptografi. Penulis mengucapkan terima kasih kepada Bapak Rinaldi Munir sebagai dosen mata kuliah ini yang telah membimbing kami dalam menyelesaikan makalah ini.

Semoga makalah yang dibuat oleh penulis ini dapat bermanfaat pada bidang keilmuan kriptografi, pengaplikasiannya pada sistem e-voting di berbagai tempat dan bagi sesiapa yang mendapatkan mafaat dari makalah ini.

Ucapan terima kasih juga kami berikan kepada seluruh pihak yang tidak dapat disebutkan satu per satu dan telah membantu penulis dalam pembuatan makalah ini sehingga dapat diselesaikan dengan baik dan tanpa halangan berarti.

REFERENCES

Anane, Rachid, Richard Freeland, and Georgios Theodoropoulos. "E-voting requirements and implementation." In E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services, 2007. CEC/EEE 2007. The 9th IEEE International Conference on, pp. 382-392. IEEE, 2007.

Bannet, Jonathan, David W. Price, Algis Rudys, Justin Singer, and Dan S. Wallach. "Hack-a-vote: Security issues with electronic voting systems." Security & Privacy, IEEE 2, no. 1 (2004): 32-37.

Bruce Schneier (2011), Cryptanalysis of SHA-1. Available from: http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html [Accessed: May 14, 2013].

Dell - Secureworks (2011), DNS Cache Poisoning - The Next Generation. Available from: http://www.secureworks.com/resources/articles/other_articles/dns-cache-poisoning/ [Accessed: May 14, 2013].

Gritzalis, Dimitris, ed. Secure electronic voting. Dordrecht: Kluwer Academic Publishers, 2003.

Ikonomopoulos, Spyros, Costas Lambrinoudakis, Dimitris Gritzalis, Spyros Kokolakis, and Kostas Vassiliou. "Functional requirements for a secure electronic voting system." In Security in the Information Society, pp. 507-519. Springer US, 2002.

Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. "Analysis of an electronic voting system." In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pp. 27-40. IEEE, 2004.

Mamdudi, Syaugi, and Aciek Ida Wuryandari. "Sistem Keamanan Data e-Voting Menggunakan Algoritma Kriptografi Rijndael." Jurnal Sarjana ITB bidang Teknik Elektro dan Informatika 1, no. 2 (2012).

Manuel, Stéphane. "Classification and generation of disturbance vectors for collision attacks against SHA-1." Designs, Codes and Cryptography 59, no. 1-3 (2011): 247-263.

Mu, Yi, and Vijay Varadharajan. "Anonymous secure e-voting over a network." In Computer Security Applications Conference, 1998. Proceedings. 14th Annual, pp. 293-299. IEEE, 1998.

Preneel, Bart. "Analysis and design of cryptographic hash functions." PhD diss., Katholieke Universiteit te Leuven, 1993.

Rinaldi Munir, Kriptografi., Bandung: Informatika Bandung, 2006.

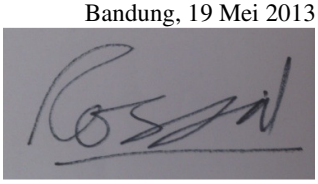
Rivest, Ronald L. "Electronic voting." In Financial Cryptography, vol. 1, pp. 243-268. 2001.

Shalahuddin, Muhammad. "Pembuatan Model e-Voting Berbasis Web (Studi Kasus Pemilu Legislatif dan Presiden Indonesia)." PhD diss., Tesis Magister, Institut Teknologi Bandung, 2009.

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, 19 Mei 2013



Abdurrosyid Broto Handoyo
13510107