Analisis Keamanan Protokol *E-auction*

Rudianto [1)]

1) Jurusan Teknik Informatika ITB, Bandung 40116, email : if14099@students.if.itb.ac.id

Abstract **–** Seiring dengan perkembangan jaman, banyak proses bisnis yang dilakukan secara elektronik. Salah satunya adalah *e*-auction, atau proses pelelangan elektronik. Meningkatkan performansi adalah kunci utama mengapa teknologi ini menjadi sangat disukai sedangkan faktor keamanan masih menjadi sebuah ketakutan tersendiri untuk calon pengguna. Akhir-akhir ini banyak teknik-teknik kriptografi yang digunakan untuk mengamankan sistem *e-auction*. Dalam makalah ini akan diperbandingkan teknik-teknik kriptografi yang telah ada, beserta keuntungan dan kerugiannya serta *requirement* apa yang dibutuhkan oleh sebuah sistem *e-auction.*

Dalam proses pengamanan *e-auction* ada beberapa skema *receipt-free* yang ditawarkan yang masing-masing memiliki spesifikasi yang khusus untuk mencegah kecurangan-kecurangan dalam proses pelelangan. Kecurangan dalam hal ini biasanya berupa "*man in the middle" attack* yang dilakukan terhadap protokol. Salah satu kakas yang bersifat *open-source* dan biasa digunkan untuk mengetahui kekuatan protokol *e-auction* adalah AVISPA (Automated Validation of Internet Security Protocol and Application).

Kontribusi yang dilakukan oleh penulis dimulai dari studi literatur mengenai apa itu *e-auction,* apa keuntungannya, bagaimana aplikasinya, teknik-teknik kriptografi yang digunakan untuk mengamankan sistem ini serta serangan yang dilakukan terhadap protokol *e-auction.* Selain itu penulis juga akan menganalisis tingkat keamanan teknik-teknik kriptografi yang ada berdasarkan beberapa kasus. Penulis juga akan mencoba langsung sistem *e-auction* situs jalintrade. Kemudian penulis akan menganalis proses yang terjadi di dalamnya untuk mencari celah keamanan, serta mencoba melakukan serangan pada dengan seijin administrator dari situs tersebut dan menganalisis hasilnya. Jika ada kekurangan, maka penulis akan mencoba menawarkan usulan baru.

Kata Kunci*: e-auction, keamanan, kriptografi, protokol, kunci privat, kunci public, lelang*

1. PENDAHULUAN

Akhir-akhir ini, seiring dengan perkembangan teknologi komunikasi dan informasi, segala kegiatan mulai dikaitkan dengan proses elektronik, yang biasa disebut dengan "*e-anything*", seperti *e-government, e-banking, e-learning, e-auction*, dll. Hal ini disebabkan karena proses elektronik dapat meningkatkan *availability* dari konsumen terhadap sistem serta dapat memangkas biaya yang diperlukan, jika dibandingkan dengan cara tradisional.

Aplikasi *Electronic Auction* atau yang biasa disingkat *e-auction* merupakan sebuah aplikasi untuk mengelola proses pelelangan, baik lelang jual maupun lelang beli, yaitu untuk melakukan penawaran harga dari peserta lelang berbasis internet yang dirancang untuk mencapai suatu proses pelelangan yang transparan, efektif, efisien, dan terintegrasi.

Dalam istilah pelelangan, pihak yang akan menjual barang / jasa sering disebut pelaksana lelang, sedangkan pihak yang berfungsi sebagai calon pembeli disebut peserta lelang. Istilah lainnya adalah lelang jual dan lelang beli. Lelang jual (*auction*) adalah proses pelelangan yang dilakukan oleh pelaksana lelang untuk menjual barang/jasa kepada peserta lelang. Sedangkan lelang beli (*reverse auction*) adalah proses pelelangan yang dilakukan oleh pelaksana lelang untuk mengadakan / membeli barang / jasa dari pihak pelaksana lelang. Secara umum, pelelangan memiliki 4 tipe, yaitu : skema "*English auction*" (pengguna dapat menawar berulang kali, sampai tidak ada bisa menawar lebih tinggi, penawaran tertinggi menang), skema "*first sealed bid*" (hanya sekali melakukan penawaran, yang tertinggi menang), skema "*second price sealed bid*" (hanya sekali melakukan penawaran, yang tertinggi menang dan membayar seharga penawaran tertinggi kedua), dan skema "Dutch auction" (harga terus menurun sampai ada yang bersedia membeli).

Untuk *e-auction,* di luar negri sudah banyak situs yang populer, contohnya eBay, sedangkan di dalam negri masih sedang dikembangkan oleh pihak PT. Telkom. Dalam sebuah artikel yang diterbitkan dalam situs resminya, PT. Telkom menyatakan bahwa *e-auction* memiliki prospek yang sangat cerah di masa depan dan dapat menghasilkan keuntungan yang sangat besar dalam proses tender perusahaan. Salah satu faktor yang penting untuk keberlangsungan sistem ini adalah faktor keamanan. Salah satu situs *e-auction* yang sedang dikembangkan oleh PT. Telkom adalah JalinTrade, yang menggunakan skema 'English auction", dan digunakan sebagai objek dalam makalah ini. Perlu ditekankan bahwa situs ini belum memiliki intensitas transaksi yang tinggi karena masih dalam tahap perkembangan, pengujian dilakukan atas izin dari administrator situs, serta semua pengujian yang dilakukan tidak berbahaya bagi sistem tersebut. Dalam melakukan serangan "*man in the middle*" penulis berperan sebagai korban dan penyusup sekaligus dengan cara membuat sebuah website tiruan dengan tampilan seadanya yang hanya mengutamakan proses penyadapan pesan rahasia.

2. KEAMANAN PROTOKOL E-AUCTION SITUS E-AUCTION JALINTRADE

Protokol keamanan *e-auction*

Protokol keamanan dalam *e-auction* harus dapat menjamin beberapa faktor antara lain :

- *Privacy* : tidak ada orang lain selain peserta lelang itu sendiri dan pihak pelaksana lelang yang dapat melihat isi dari tawaran yang dikirimkan, kecuali tawaran pemenang.
- Kerahasiaan peserta lelang : identitas sebenarnya dari pemenang dari proses lelang tidak dipublikasikan.
- Integritas data : data yang dikirim dan data hasil akhir tidak dapat dimodifikasi.
- Keamanan tawaran : tawaran tidak dapat dipalsukan atau disadap.
- Nir-penyangkalan : peserta lelang tidak dapat menyangkal bahwa ia telah melakukan tawaran.
- Autentifikasi partisipan : hanya yang telah terdafta yag dapat mengikuti proses pelelangan.
- Verifikasi publik ; setiap orang bisa mengecek tawaran mana yang memenangkan pelelangan.
- *Robustness* : jika peserta lelang mengirimkan tawaran yang salah maka sistem tidak akan terpengaruh.
- *Receipt freeness* : semua orang termasuk tidak melakukan pembuktian tentang informasi tawaran kepada pihak manapun karena sudah ditangani oleh sistem.

Pengenalan Situs JalinTrade

Objek dalam makalah ini adalah sebuah situs komersil jalintrade yang dikembangkan oleh PT. Telkom yang bekerja sama dengan perusahaan asing Commerce One. Situs ini terdiri dari beberapa modul, antara lain :

- Modul Pra Auction

Modul ini digunkanan oleh pihak pelaksana lelang untuk menentukan spesifikasi pelelangan (jenis barang yang akan dilelang, harga awal, waktu lelang, dll), menentukan peserta lelang, serta untuk menyetujui spesifikasi pelelangan yang direncanakan.

- Modul Monitoring

Modul ini digunakan oleh pihak pelaksana lelang untuk memantau pergerakan harga penawaran yang dimasukkan oleh peserta lelang.

- Modul Reporting

Modul ini digunakan oleh pihak pelaksana lelang untuk mencetak data hasil penawaran harga peserta lelang.

- Modul Pemenang

Modul ini digunakan untuk menentukan pemenang lelang.

- Modul Manajemen Auction

Modul ini digunakan oleh pihak pelaksana lelang untuk mengelola pelaksanaan pelelangan, yaitu untuk mengulang pelaksanaan lelang, menghapus data yang salah, mengaktifkan kembali data yang salah hapus, memperpanjang waktu lelang, dll.

- Modul Auction

Modul ini digunkanan oleh pihak peserta lelang untuk memasukkan harga penawaran.

- Modul Admin

Modul ini digunakan oleh pihak Administrator untuk mengelola pengguna aplikasi ini.

Gambaran sistem jalintrade

Berikutnya, untuk penyederhanaan penulisan entitas yang ada akan digunakan singkatan:
A sebagai pihak pelaksana lelang
B sebagai pihak peserta lelang
C sebagai pihak jalintrade
WWW sebagai halaman tampilan

Protokol kriptografi akan situs ini terdiri dari empat subprotokol yaitu : pembuatan sertifikat, notifikasi pelelangan, notifikasi tawaran, serta pilihan dari tawaran. Langkah pertama adalah registrasi calon pengguna untuk dapat mengakses situs tersebut. Untuk keperluan penelitian penulis mendaftarkan pengguna baru dengan spesifikasi :

user name	:	Rudianto
password	:	kripto
company	:	EXE

Subprotokol pembuatan sertifikat digunakan oleh seluruh D. Langkah berikutnya aalah notifikasi pelelangan oleh A dimana C mempublikasikan pengumumanan bahwa ada pelelangan barang / jasa milik A beserta spesifikasinya. Berikutnya, setiap D dapat ambil bagian dalam lelang ini dengan mengirimkan tawarannya ke C. Subprotokol terakhir dilakukan ketika proses pelelangan selesai ketika waktu lelang yang ditentukan telah berakhir. Kemudian A dan para penawar mengirimkan pesan rahasia ke C sebagai validasi. Setelah mendekripsi pesan rahasia tersebut, C mengirimkannya ke A, pihak yang akan menentukan tawaran yang menang dan mengirimkan datanya kembali ke C. Akhirnya C mengumumkan nomor tawaran yang memenangkan pelelangan tersebut melalui WWW. Berikutnya akan dijelaskan dengan lebih rinci setiap subprotokol yang ada.

- Subprotokol pembuatan sertifikat

1. $D \rightarrow C : \{SK_D\}\ PK_C$
2. $D \leftarrow C :$
   $\{\{\{NR_D\}\ SK_C,\ T_D,\ (SK_D,\ PK_D)\}SK_C\}PK_D$

Subprotokol ini bekerja sebagai berikut. Setiap orang yang ingin membuat sertifikat (D) bisa saja berupa seorang pelaksana lelang ataupun peserta lelang. Dia harus memiliki kunci privat (SK_D) dan kunci public (PK_D) yang didapatkan dari proses login. Data yang ditandatangani menggunakan kunci privat (SK_D) dan telah dienkripsi menggunakan kunci publik situs (PK_C) kemudian dikirimkan ke C. Kemudian C mendekripsi data tersebut dan bila data valid maka C akan membangkitkan suatu bilangan acak nilai

registrasi (NR_D) yang valid selama timestamp waktu yang telah ditentukan sebelumnya (T_D). C kemudian membangkitkan kunci privat dan kunci publik yang baru (SK_D dan PK_D) untuk D yang akan digunakan pada subprotokol berikutnya. Kedua kunci ini valid selama selang waktu (T_D). C menandatangani data tersebut (SK_D, PK_D, dan T_D) dengan kunci privatnya (SK_C) kemudian mengenkripsinya dengan kunci publiknya (PK_C) dan mengirimkannya ke D.

- Subprotokol notifikasi pelelangan

Subprotokol ini dirancang untuk A yang akan mengumumkan pelelangan. Prekondisinya adalah A sukses menyelesaikan protokol pembuatan sertifikat.

1. $A \rightarrow C : \{\{NR_A, T_A, AP_A, N_A\}SK_A\}PK_C$
2. $A \leftarrow C : \{\{SK_{P(A)}\}\ SK_C\}\ PK_A$
3. $C \rightarrow WWW : NB_{AU}, AP_A, PK_{AU}$

A mengirimkan data berupa nomor registrasi (NR_A), dan timestampnya (T_A) yang merupakan hasil dari subprotokol sebelumnya beserta spesifikasi pelelangan (AP_A), dan user id dari pelaksana lelang (N_A), yang telah ditandatangani menggunakan kunci privat SK_A serta telah dienkripsi menggunakan kunci publik PK_C kepada C. C kemudian melakukan verifikasi nomor registrasi (NR_A) dan timestampnya (T_A). Jika data valid maka C akan membangkitkan kunci publik dan privat khusus untuk pelelangan ini (PK_{AU} dan SK_{AU}). Kunci privat (SK_{AU}) dipecah menjadi tiga bagian yaitu $SK_{P(A)}$ untuk A $SK_{P(C)}$ untuk C dan $SK_{P(B)}$ untuk semua peserta lelang. Setiap bagian diperlukan untuk membangkitkan SK_{AU}. Kemudian C mengirimkan $SK_{P(A)}$ yang telah ditandatangani dengan SK_C serta telah dienkripsi dengan PK_A. Langkah berikutnya, C mempublikasikan nomor pelelangan tersebut (NB_{AU}), spesifikasi pelelangan (AP_A) dan kunci publik pelelangan (PK_{AU}).

- Subprotokol notifikasi tawaran

Setelah pelelangan dipublikasikan, pihak yang berminat dapat mengajukan tawaran mereka. Setiap calon peserta lelang harus memiliki nomor registrasi (NR_B), kunci privat (SK_B) dan tawarannya (OF_B), kemudian peserta lelang membangkitkan bilangan acak (NB_B) dan menandai tawaranya dengan timestamp (TOF_B).

1. $B \rightarrow C : \{\{OF_B\}\ SK_B\}\ PK_{AU}, \{\{NB_B, NR_B, NB_{AU}, TOF_B\}\ SK_B\}PK_C$
2. $B \leftarrow C : \{\{Confirmation\}\ SK_C\}PK_B$

Peserta lelang mengirimkan data (NB_B, NR_B, NB_{AU}, TOF_B) yang telah ditandatangani dengan kunci privat (SK_B) serta telah dienkripsi dengan kunci publik (PK_C). Selain itu peserta lelang juga mengirimkan tawaran (OFB) yang juga telah ditandatangani dengan kunci privat (SK_B) serta telah dienkripsi dengan kunci publik pelelangan tersebut (PK_{AU}). Jika data yang dikirimkan valid maka C akan mengirimkan konfirmasi yang telah ditandatangani dengan kunci privat (SK_C) serta telah dienkripsi dengan kunci publik (PK_B).

- Subprotokol pemilihan tawaran

Subprotokol ini dieksekusi setelah waktu pelelangan berakhir.

1. $C \rightarrow Bi : \{\{SK_{P(Bi)}\}\ SK_C\}\ PK_{Bi}$
2. $A \rightarrow C : \{\{SK_{P(A)}\}\ SK_A\}\ PK_C$
3. $C \leftarrow Bi : \{\{SK_{P(Bi)}\}\ SK_{Bi}\}\ PK_C$
4. $A \leftarrow C : \{\{\{OF_{Bi}\}, SK_{Bi}\}\ SK_C\}\ PK_A$
5. $A \rightarrow C : \{\{NR_{B(win)}, NR_A, N_{Bi}, N_A, NB_{AU}\}\ SK_A\}\ PK_C$
6. $C \rightarrow WWW : NR_{B(win)}, N_{Bi}$

Dengan mengetahui jumlah peserta lelang (N) yang mengajukan tawaran mereka, C membagi kunci privat pelelangan menjadi N bagian $SK_{P(Bi)}$. C menggunakan skema "safe threshold" dalam proses pembagiannya. Partisi kunci privat yang baru terbentuk ($SK_{P(Bi)}$) ditandatangani menggunakan kunci privat (SK_C) dan dienkripsi menggunakan kunci publik (PK_B) dan dikirimkan ke setiap peserta lelang. Langkah berikutnya, A dan Bi mengirimkan partisi kunci privatnya yang telah ditandatangani dan dienkripsi ke C. Setelah itu, C menggabungkan seluruh partisi yang ada menjadi kunci privat pelelangan (SK_{AU}). Dengan mendapatkan semua kunci, C dapat mendekripsi setiap tawaran yang diajukan (OF_B) pada protokol sebelumnya. Setelah itu, C mengirimkan semua tawaran yang ada, yang telah ditandatangani oleh masing-masing peserta lelang (Bi) ke A. Tawaran-tawaran tersebut sebelumnya didekripsi dengan kunci privat (SK_C) dan dienkripsi ulang menggunakan kunci publik (PB_A). Setelah A menerima semua tawaran yang ada, A bisa memilih tawaran mana yang paling baik dan mengirimkan hasilnya ke C. Hasil yang dikirimkan termasuk nomor registrasi peserta yang memenangkan tawaran ($NR_{B(win)}$), nomor registrasi dari pelaksana lelang (NR_A), nomor acak dari peserta yang telah mengirimkan tawaran(N_B), dan nomor pelelangan (N_{AU}). Seluruh informasi ini ditandatangani menggunakan kunci privat (SK_A) dan dienkripsi menggunakan kunci publik (PK_C). Setelah mendapatkan informasi pemenangnya, C mempublikasikan nomor acak dari peserta lelang yang menang ($NR_{B(win)}$) dan jumlah peserta lelang (N_{Bi})

3. SERANGAN KRIPTOGRAFI

Ada beberapa jenis serangan yang dapat dilakukan terhadap proses bisnis *e-auction*, antara lain :

- Authentication Breach : penyerang menjalankan protokol untuk meniru pengguna yang legal.
- Authentication Breach + Secret Retrieval : penyerang menjalankan protokol untuk meniru pengguna yang legal untuk menerima dan mengirimkan pesan rahasia.
- Authentication Breach + Secret Revival : penyerang menjalankan protokol untuk meniru pengguna yang legal untuk mengambil pesan rahasia yang lama.
- Authentication Breach + Secret Injection : penyerang menjalankan protokol untuk meniru pengguna yang legal untuk menambahkan pesan rahasia yang baru.

- Message Generation : penyerang menjalankan protokol sampai suatu tahapan dimana ia dapat memperoleh pesan rahasia baru yang valid tetapi palsu.
- Secret Retrieval : penyerang mengambil pesan rahasia yang disebarkan antara dua pengguna.
- Session hijacking : pengguna mengambil alih jalannya protokol setelah kedua pihak telah diautentifikasi dan sebelum pesan rahasia diterima oleh pihak penerima.

Serangan yang coba dilakukan oleh penulis adalah "man in the middle". Dalam hal ini penulis membuat sebuah tiruan sederhana dari situs jalin trade ini dengan tampilan yang seadanya. Ini didasarkan pada fakta bahwa pesan yang dikirimkan oleh D dan C pada subprotokol pertama tidak diautentifikasi dan berdasarkan fakta bahwa jawaban yang diberikan oleh *server* tidak mengadung informasi mengenai identifikasi dari D.
Keterangan :
I : penyusup,
I(D) : I menyamar sebagai D

1. $D \rightarrow I(C) : \{SK_D\}\ PK_C$
2. $I(D) \rightarrow C : \{SK_I\} PK_C$
3. $I(D) \leftarrow C :$
   $\{\{NR_I\}\ SK_C, TNR_I, \{SK_I, PK_I\}\ SK_C\}\ PK_I$
4. $\leftarrow I(C) :$
   $\{\{NR_I\}\ SK_C, TNR_I, \{SK_I, PK_I\}\ SK_C\}\ PK_D$

Serangan ini memerlukan dua session dari subprotokl yang pertama. D memulai langkah 1 dari session ini dan mulai mengirimkan pesan. Penyusup mengendalikan jaringan dan memblok pesan pertama yang dikirmkan oleh C. Secara bersamaan, penyerang melakukan langkah 2 pada session yang berbeda dengan server C. Penyusup membangkitkan data baru dan bukan data yang dibangkitkan oleh D pada langkah pertama. D secara otomatis membangkitkan nomor registrasi, timestamp, dan pasangan kunci baru yang ditandatangani dengan kunci privatnya dan dienkripsi dengan kunci publik dari penyusup. Penyusup mendekripsi pesan itu dengan kunci privatnya dan mendapatkan pasangan kunci baru dari server. Sekarang penyusup dapat memalsukan pesan pada langkah 4 untuk meyakinkan D bahwa semuanya baik-baik saja. Karena penyusup dapat mengerti pertukaran informasi terenkripsi antara C dan D maka untuk proses berikutnya dapat dengan mudah "dikerjai".

4. HASIL DAN PEMBAHASAN

Hasil percobaan

Karena situs ini masih berbasis pada pola protokol yang seperti dijabarkan sebelumnya maka serangan berhasil dilakukan dengan baik dimana pertukaran informasi antara server dan pengguna sudah dapat dimanipulasi.

Hasil pengamatan

Ada sebuah bagian dari subprotokol tersebut yang dirasakan kurang perlu, yaitu pada bagian dimana setiap peserta lelang akan mendapatkan partisi dari kunci privat lelang. Hal ini dapat mengakibatkan kegagalan jika ada salah satu saja partisi yang rusak / hilang.
Penggunaan digital signature untuk masing pesan yang dikirim dirasakan kurang efektif dan tidak diperlukan karena hanya dengan pasangan kunci publik-pivat untuk enkripsi dan dekripsi saja sudah cukup untuk mengautentifikasikan pengguna.

Solusi

Beberapa perubahan yang perlu dilakukan antara lain :
- Tidak lagi memerlukan digital signature
- Nomor registrasi dan timestamp kini bergantung pada data apa yang dikirimkan.
- Ada penambahan sebuah langkah sebagai suatu jaminan bahwa penerima pesan telah menerima pesannya dengan baik dan menghindari kemungkinan pengirim pesan berkomunikasi dengan penyusup yang menyamar menjadi penerima pesan sebagai konfirmasi ulang.
- Identitas dari server (C), pelaksana lelang (A), atau peserta lelang (B) harus selalu disertakan dalam setiap pertukaran informasi untuk untuk menghindari kemungkinan serangan "*man in the middle*".
- Penambahan fungsi hash untuk menjaga bahwa C tidak dapat mengetahui isi dari tawaran-tawaran yang ada.

  Setelah mengalami revisi, protokol yang ada menjadi :

- Subprotokol pembuatan sertifikat :

1. $D \rightarrow C : \{D, N_D\}\ PK_C$
2. $D \leftarrow C :$
   $\{N_D, NR_D, TNR_D, C\}PK_D$
3. $D \rightarrow C : \{D, NR_D\}\ PK_C$

Client (D) mengirimkan identitasnya dan bilangan acak (N_D) yang dienkripsi dengan kunci publik server (PK_C). Server menjawab dengan mengirimkan pesan yang berisi : bilangan acak milik client (N_D), nomor register yang baru (NR_D), timestamp (TNR_D) dan dienkripsi dengan menggunakan publik key client(PK_D). Akhirnya client mengkonfirmasi dengan mengirimkan ke server nomor registrasinya yang dienkripsi dengan kunci publik server (PK_C).

- Subprotokol notifikasi pelelangan

1. $A \rightarrow C : \{NR_A, T_A, AP_A, N_A, A\}\ PK_C$
2. $A \leftarrow C : \{N_A, NB_{AU}, C\}\ PK_A$
3. $A \rightarrow C : \{NB_{AU}, TNB_{AU}\}\ PK_C$
4. $C \rightarrow WWW : NB_{AU}, T_{AU(open)}, T_{AU(close)}, AP_A, PK_{AU}$

Dalam fase ini, A memasukkan pelelangannya ke

server. Pada awalnya A mengirimkan pesan yang berisi nomor registrasi (NR_A) yang didapatkan dari subprotokol sebelumnya, spesifikasi dari lelang (AP_A) dan identitasnya (A) serta sebuah bilangan acak baru (N_A). Pesan ini diekripsi menggunakan kunci yang didapat dari C. Server kemudian mengecek validitas dari nomor registrasi dan bila valid akan membangkitkan bilangan acak baru (NB_{AU}). Kemudian C mengirimkan nomor pelelangan (NB_{AU}) dan timestampnya (T_{NBAU}) dan identitasnya ke B kemudian mempublikasikan ke situs waktu mulai dan waktu selesai pelelangan terserbut

- Subprotokol notifikasi tawaran

1. B → C : $\{NR_B, NB_{AU}, B, N_{OFB}, \{OF_B\} PK_A, h(OF_B)\} PK_B$
2. B ← C : $\{NB_{OFB}, N_{OFB}, C\} PK_B$
3. B → C : $\{NB_{OFB}, T_{NBOFB}\} PK_{TTP}$

B mengajukan tawaran (O_{FB}) dan membangkitkan bilangan acak (N_{OFB}). Ia mengenkripsi dengan kunci publik C dan mengirimkan pesan ke A yang berisi nomor pelelangan (NB_{AU}), identitas (B), dan bilangan acak baru (N_{OFB}), dan tawarannya. Tawarannya dienkripsi terlebih dahulu dengan kunci publik (PK_A) untuk mencegah C dapat mengetahui isi tawaran dan kemudian di hash untuk mencegah kemungkinan C dapat mengetahui identitas B pada subprotokol terakhir. Server menjawab dengan memberikan nomor registrasi bary (NB_{OFB}), bilangan acak yang diterima dari B (N_{OFB}) dan identitasnya. B melakukan konfirmasi dengan cara mengirimkan nomor registrasi dan timestampnya (NB_{OFB} dan T_{NBOFB})

- Subprotokol pemilihan tawaran

Subprotokol ini dieksekusi setelah waktu pelelangan berakhir.

1. A ← C : $\{NB_{AU}, \{O_{FBi}\} PK_A, C, N_C\} PK_A$
2. A → C : $\{h(OFB(win)), NB_{AU}, N_C, A\} PK_C$
3. C → WWW : $N_{OFB(win)}, N_{OFBi}, NB_{AU}$

Bagian ini mengalami banyak penyederhanaan karena dirasakan kurang perlu untuk diterapkan. C mengirim pesan ke A yang berisi nomor pelelangan (NB_{AU}), semua tawaran (O_{FBi}) yang dienkripsi dengan kunci publik (PK_A), identitasnya, serta bilangan acak baru. Seluruh pesan tersebut dienkripsi dengan kunci publik (PK_A). A menentukan tawaran mana yang memenangkan dan mengirimkan pesan ke C yang berisi tawaran pemenang yang telah di hash, bilangan acak yang berasal dari C, serta identitasnya. Akhirnya menggunakan hash dari tawaran yang ada di subprotokol sebelumnya, C menemukan dan mempublikasikan nomor pemenang lelang ($NB_{OFB(win)}$), seluruh nomor peserta lelang (N_{OFBi}), dan nomor dari pelelangan (NB_{AU}). Langkah ini memastikan bahwa semua pengajuan tawaran yang dilakukan oleh semua peserta lelang sudah diterima oleh pihak pelaksana lelang sekaligus semua orang dapat mengecek siapa pemenang dari pelelangan ini.

Analisis Keamanan

- Kerahasiaan : Integritas dan realibilitas dari tiap transaksi harus terlindungi, kecuali informasi yang dipublikasikan ke situs. Setiap pesan yang dikirim harus dienkripsi dengan kunci publik. Untuk mengecek faktor ini dapat menggunakan kakas OMFC yang merupakan bagian dari AVISPA.
- Autentifikasi : Hanya orang yang terdaftar yang dapat membuat sebuah pelelangan dan mengajukan tawaran. Subprotokol pembuatan sertifikat yang bertanggung jawab penuh terhadap faktor ini.
- Nir-penyangkalan : Pemenang dan pelaksana lelang tidak bisa menyangkal isi dari tawaran mereka karena ada identitas dalam setiap pengirimannya.
- Kerahasiaan dari peserta lelang : Hal ini didukung oleh pernyataan bahwa hanya nomor yang berasosiasi dengan peserta lelang yang dipublikasikan oleh server dan nomor tersebut bersifat berbeda untuk tiap proses lelang.

5. KESIMPULAN

E-auction merupakan fitur yang sangat berguna untuk meningkatkan performansi dari proses lelang tradisional. Faktor keamanan dari *e-auction* adalah bagian yang paling penting. Banyak faktor yang harus dipenuhi untuk memenuhi standar ini, antara lain : privacy, autentifikasi, nir-penyangkalan, dll. Ada beberapa jenis serangan yang dapat dilakukan ke sistem, salah satunya adalah "*man in the middle*" attack yang digunakan pada makalah ini.

Situs jalintrade yang dijadikan sebagai objek dari analisis keamanannya memiliki protokol yang terbagi menjadi beberapa subprotokol antara lain : pembuatan sertifikat, notifikasi pelelangan, notifikasi tawaran, dan pemilihan tawaran. Masing-masing protokol tersebut memiliki proses keamanan yang berlapis.

Pengujian dengan serangan "*man in the middle*" dilakukan terhadap situs ini dan berhasil mengubah informasi yang dikirmkan oleh pengguna. Berdasarkan pengujian tersebut dapat ditarik kesimpulan bahwa ada beberapa kekurangan yang ditemui setelah melalui proses analisis. Sistem ini ternyata sangat rentan terhadap serangan "man in the middle" karena tidak ada proses identifikasi identitas dari pengirim pesan. Beberapa faktor pengaman juga dirasakan tidak diperlukan untuk mengurangi beban komputasi dan juga sistem ini.

Untuk mengatasi hal tersebut diadakan beberapa perubahan pada keempat subprotokol tersebut.

Penghilangan proses penandatangan digital. Nomor registrasi dan timestamp kini bergantung pada data apa yang dikirimkan. Penambahan langkah konfirmasi pada akhir setiap protokol. Pengiriman identitas untuk menghindari kemungkinan serangan "*man in the middle*". Penambahan fungsi hash untuk menjaga kerahasiaan tawaran.

DAFTAR REFERENSI

[1] Munir, Rinaldi, Ir.,M.T. 2007. *Diktat Kuliah IF-5054 Kriptografi*. Informatika-ITB : Bandung.
[2] http://www.zamrudtechnology.com/files/editor/File/Flyer_SpOffring/eAuction_EE.pdf
[3] http://www.telkom.net/pojok_e_telkom_eauction.php
[4] http://thor.info.uaic.ro/~fltiplea/CC/CCCourseObj.html
[5] http://www.inf.ethz.ch/research/disstechreps/theses/index.htm
[6] http://www.cs.ucf.edu/~tiplea/IntroductionToCryptography.pdf
[7] http://jalintrade.com (kasus uji *e-auction*)
[8] http://avispa-project.org (kakas pengujian keamanan protokol)