`PERANGKAT LUNAK IMPLEMENTASI COMMON PASSWORD MENGGUNAKAN SHA DAN PSEUDO NUMBER RANDOM GENERATOR

Megah Mulya
Fakultas Ilmu Komputer Universitas Sriwijaya

ABSTRAK

Saat ini telah banyak terjadi kejahatan yang berakibat terbongkarnya akun-akun rahasia oleh pihak-pihak yang tidak memiliki hak akses dengan cara mencuri password.. Apalagi jika pengguna memiliki berbagai akun dengan password yang berbeda-beda agar password aman. Selama ini sudah ada metode untuk membantu pengguna dalam mengingat akun dan password yang biasa dikenal dengan *cookies*. Akan tetapi metode ini memiliki Kelemahan yaitu pengguna harus selalu memakai komputer yang sama dan komputer tidk boleh digunakan pihak lain agar password terjaga kerahasiaannya. Oleh karena itu diperlukan suatu metode untuk mengamankan berbagai password tersebut dengan tetap memberikan kemudahan bagi pengguna. Penelitian ini mengusulkan suatu metode yang kegunaannya seperti halnya *cookies* namun dengan meningkatkan sisi keamanan dan kepraktisan. Penelitian ini tidak menggunakan algoritma kriptografi kunci simetri maupun asimetri dalam pengamanan pasword akan tetapi menggunakan algoritma fungsi *hash* SHA dan pembangkit bilangan acak (pseudo number random generator/PNRG). PNRG digunakan untuk menghasilkan bilangan acak yang terkendali yang akan digabungkan dengan password diproses dengan SHA menjadi *message digest.*Bilangan acak yang telah disisipkan dalam password berfungsi sebagai kunci otentikas. M*essage digest* yang dihasilkan oleh SHA kemudian disimpan didalam basis data. Metode tersebut telah berhasil diimplementasikan kedalam perangkat lunak berbasis web dan dapat diakses secara online

Kata kunci : pasword, cookies, *malicious server attack*

PENDAHULUAN

Pada saat ini penggunaan internet sudah merupakan hal yang semakin umum. Terdapan berbagai sumber daya yang ada di internet misalnya email, facebook, twiter dan lain sebagainya yang dapat dimanfaatkan oleh masyarakat umum. Demi menjaga kerahasiaan, hak akses, keotentikan dan lain sebagainya maka sumberdaya-sumberdaya tersebut dilindungi dengan menggunakan pasangan akun dan pasword. Sehingga saat ini sudah menjadi hal yang umum jika pengguna internet memiliki lebih dari satu email, facebook dan lain sebagainya. Sudah menjadi standar bahawa berbagai akun tersebut masing-masing dilindungi dengan password. Berbagai akun tersebut sangat disarankan agar dillindungi dengan password yang berbeda-beda. Hal itu dimaksudkan untuk mencegah agar jika rahasia password suatu akun berhasil diserang(diketahui) oleh pihak lain maka pasword yang lain bisa tetap aman.

Kondisi kepemilikan banyak akun dengan pasword yang berbeda-beda berdampak pengguna terbebani untuk dapat menghafal seluruh pasword tersebut agar tidak lupa bunyi frasenya dan juga jangan sampai tertukar satu dengan yang lainnya. (Luo dan Henry, 2003). Sudah banyak terjadi di dunia internet banyak kejahatan yang berakibat terbongkarnya akun-akun rahasia oleh pihak-pihak yang tidak memiliki hak akses dengan cara mencuri password.

Selama ini sudah ada metode untuk membantu pengguna dalam mengingat *username* dan *password* yang biasa dikenal dengan *cookies*. Metode ini memanfaatkan struktur daya yang kecil yang digunakan oleh web server untuk mengirim data ke browser client (Avestro, 2007). Akan tetapi metode ini memiliki kelemahan dalam keamanan

dan kepraktisan. Kelemahannya adalah *password* masih dapat dengan mudah dicuri jika komputer digunakan oleh pihak lain. Selain itu pengguna harus selalu menggunakan komputer yang sama agar dapat memanfaatkan bantuan *cookies*. (Luo dan Henry, 2003).

Penelitian ini mengusulkan suatui metode yang kegunaannya seperti halnya *cookies* namun dengan meningkatkan sisi keamanan dan kepraktisan. Sehingga dapat memberikan keamanan dan kenyamanan bagi pengguna untuk mereduksi beban dalam mengelola banyak pasangan *username* dan *password*. Metode yang digunakan dalam penelitian ini berupa password bersama (*common password*) yang diimplementasikan dalam sebuah perangkat lunak online.

LANDASAN TEORI

A. Metode Password Bersama

Pasword diperlukan untuk kunci dalam proses otentikasi. Terdapat dua jenis otentikasi yaitu *entity authentication* dan *message authentication*. *Entity authentication* (keaslian entitas : user, terminal komputer atau kartu kredit), yang memiliki arti keaslian identitas pemilik data/pesan. Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan: "Apakah pihak yang diajak berkomunikasi/mengakses sistem adalah benar-benar pihak yang dikehendaki (yang dipercaya) ?" .

Terdapat jenis otentikasi lain yaitu *Message authentication* (keaslian pesan) berarti bukti bahwa pesan benar-benar berasal dari pengirim yang sesungguhnya dalam komunikasi, atau diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima tidak mengalami perubahan (modifikasi) selama ditransmisikan ?". Masalah keaslian pesan berkaitan dengan keutuhan pesan (*data integrity*), hal itu disebabkan pemalsuan pesan dapat diketahui dengan cara melakukan pengecekan terhadap keutuhan pesan(perubahan terhadap pesan).

Password selalu dihubungan dengan istilah *secure* yang berarti aman. Kondisi aman tidak akan dapat tercapai secara sempurna (100% aman) akan tetapi terdapat batasan sehingga kondisi tertentu dianggap aman. Kondisi aman yang dimaksud adalah jika usaha yang diperlukan untuk mengetahui suatu informasi lebih besar daripada nilai informasi yang didapat. Dengan begitu, semakin penting informasi yang ingin diamankan maka semakin besar pula usaha yang harus dilakukan untuk mendapatkan informasi tersebut.

Pasword bersama merupakan sebuah pasword yang dijadikan pedoman untuk membangkitkan password khusus (*specific*). Adapun pasword khusus merupakan hasil transformasi dari pasword bersama dan dapat dihitung dengan cara sebagai berikut;

$$Pk = T(H(Pb \ \& \ n))$$

Dimana *Pk* adalah pasword khiusus, *Pb* adalah pasword bersama, H(●) merupakanfungsi hash satu arah, n adalah bilangan bulat 1,2,3...dan seterusnya, sedangkan tamda & merupakan operator konkatenan yang berfungsi menyambung dua buah string. Bilangan n menentukan urutan pasword khusus. Sebagai contoh jika terdapat lima buah pasword khusus maka kelima pasword khusus memiliki n berupa angka 1,2,3,4 dan 5. Angka bulat yang akan digabung (*concat*) dengan password tersebut dihasilkan oleh psudo number random generator (PNRG).

a) SHA

SHA merupakan singkatan dari *Secure Hash Algorithm* yang dirancang oleh *National Institute of Standards and Technology* (NIST) bersama dengan *National Security Agency* (NSA). Tahun 1993. SHA termasuk jenis fungsi *hash*. Fungsi *hash* memetakan pesan M dengan panjang berapapun menjadi nilai hash h dengan panjang tetap (tertentu, tergantung algoritmanya). Fungsi hash mempunyai sifat-sifat sebagai berikut :

(1). h mudah dihitung bila diberikan M.

Sifat ini merupakan keharusan, karena jika h sukar dihitung, maka fungsi hash tersebut tidak dapat digunakan.

(2). M tidak dapat dihitung jika hanya diketahui h.

Sifat ini disebut juga *one-way function*, atau mudah untuk menghitung h dan sukar untuk dikembalikan ke M semula. Sifat ini sangat penting dalam teknik kriptografi, karena jika tanpa sifat tersebut maka penyerang dapat menemukan nilai M dengan mengetahui nilai *hash*-nya h.

(3). Tidak mungkin dicari M dan M' sedemikian sehingga H(M)=H(M').

Sifat ini disebut juga *collision free*. Sifat ini mencegah kemungkinan pemalsuan.

Sebagai bagian dari jenis fungsi *hash* SHA mengalami revisi pada tahu 1995, yang dikenal sebagai SHA-1. Rancangan SHA didasarkan pada algoritma MD4. Algoritma SHA-1 menerima masukan dengan panjang maksimal 2^{64} bit . Terdapat jenis serangan yang ditujukan khusus untuk fungsi *hash* selain *bruteforce attact* yaitu *birthday attack*. Akibat dari serangan ini maka kompleksitas pembongkaran nilai hash menjadi setengah dari *bruteforce attact* atau setengah dari panjang keluaran fungsi *hash*. Untuk SHA-1, maka kompleksitas yang dihadapi oleh *birthday attack* adalah $2^{160/2}$ atau 2^{80}

b) Pseudo Random Number Generator (PNRG)

Pseudo randon number generator adalah algoritma yang berfungsi untuk membuat (membangkitkan) bilangan acak secara terkendali. Terdapat berbagai algoritma pembangkit bilangan acak namun yang memiliki karakteristik komputasi yang paling sederhana sehingga memiliki performansi paling tinggi adala linear congruental generator (LCG). LCG memang bukan paling kuat untuk keperluan kriptografi namun tetap akan aman jika diacak lagi dengan algoritma yang lainnya.

Rumus matematika untuk generator bilangan acak adalah sebagai berikut:

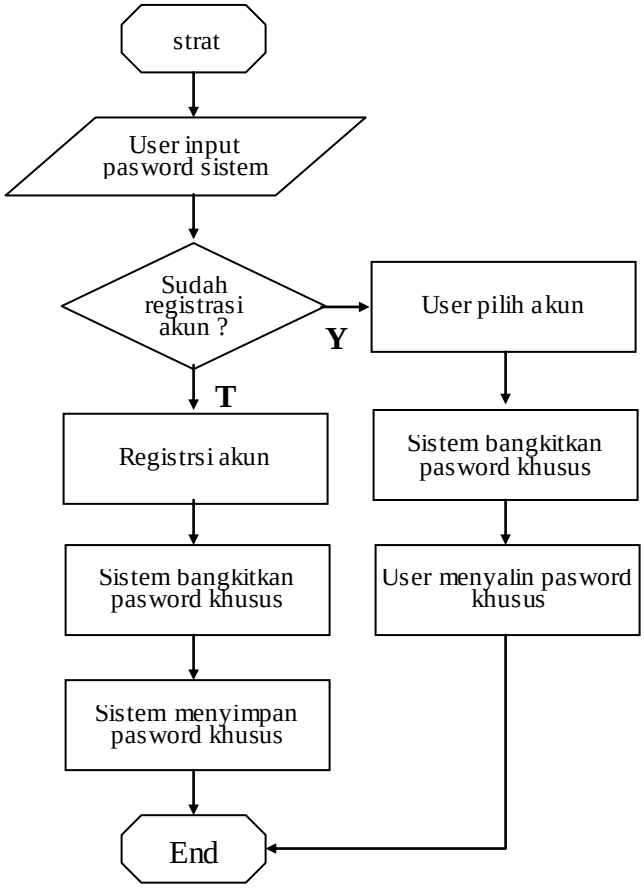
$$X_{n+1} = (a\, X_n + c)\ (\text{mod } m)$$

Dimana X akan menjadi deret niali acak dan
m, 0<m, adalah modulus
a, 0<a<m adalah konstanta
c, 0<c<m, adalah konstanta incremen
X0, 0<X<m, adalah suatu nilai awal

METODE PENELITIAN

Tahapan-tahapan dalam metode penelitian yang digunakan dalam usulan penelitian ini yaitu 1) Pengumpulan data, 2) Analisa data untuk pemodelan; 3) Analisis kebutuhan perangkat lunak, 4) Perancangan perangkat lunak dan antar muka; 5) Pengkodean perangkat lunak, 6) Pengujian perangkat lunak, dan 7) Keluaran.

.Mekanisme pengamanan *password* diilistrasikan oleh gambar 3.1 yang merupakan diagram alir dari sistem yang akan dibuat. Pada gambar tersebut dapat dilihat urutan proses yang akan dilakukan oleh sistem



Gambar .1 .Diagram alir sistem

Pada gambar 3, terdapat dua sub proses yaitu otentikasi pengguna dan membangkitkan *specific password*. Pada sub proses pertama akan dilakukan otentikasi pengguna yaitu dengan cara mencocokkan nilai *hash* pasword bersama pengguna dengan nilai *hash* yang ada di dalam server. Pada sub proses kedua sistem akan membangkitkan *specific password* yang telah dipilih oleh pengguna.

HASIL DAN PENGUJIAN PERANGKAT LUNAK

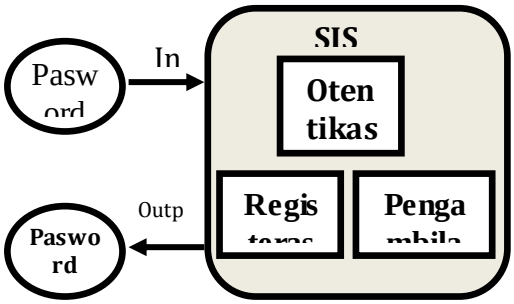
Penelitian ini mengahasilkan perangkat lunak yang dikembangkan dengan fase-fase analaisis dan perancangan yang telah diimplementasikan dan dilakukan pengujian. Pada bagian ini akan disajikan laporan hasil analisis dan perancangan perangkat lunak dan hasil pengujiannya.

A. Analisa Penerapan SHA.

Pada penelitian ini pemilihan fungsi *hash* sebagai algoritma pengacakan yang tidak dapat kembali (satu arah) disebabkan pertimbangan kepraktisan dan menghindari agar seminimal mungkin penyimpanan variabel yang berkaitan dengan pasword kedalam basis data. Dengan demikian maka dapat mengurangi resiko terbongkarnya pasword dari sisi penyimpanan dalam basis data. Algoritma fungsi *hash* yang dipilih dalam penelitian ini adalah SHA. SHA merupakan perbaikan (berbasis) dari MD4, karena MD4 sudah diketahui dapat dipatahkan oleh *cryptanalyst*. Selain itu didalam jajaran fungsi *hash* SHA mempunyai kecepatan yang paling besar. Dengan demikian maka dari aspek kekuatan SHA dan sekaligus kecepatan, SHA dapat dijadikan pilihan yang baik untuk digunakan

B. Hasil Pemodelan

Hasil pemodelan sistem perangkat lunak dapat dilihat pada gambar 5.1.

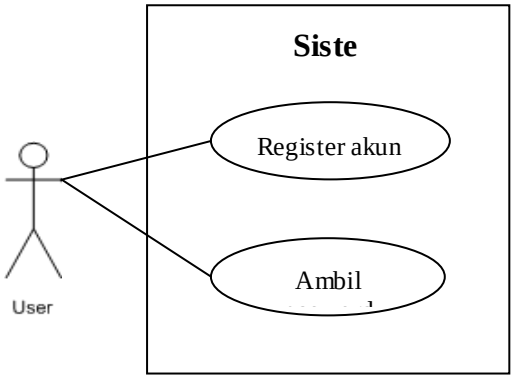


Gambar 3 Model sistem perangkat lunak

C. Hasil Implementasi Model Kedalam Perangkat Lunak

a) Spesifikasi Kebutuhan Perangkat Lunak

Spesifikasi kebutuhan perangkat lunak sebagai hasil implementasi pemodelan sistem yang telah dihasilkan pada tahapsebelumnya disajikan dalam bentuk diagram usecase seperti tampak pada gambar. Pada gambar tersebut tampak sistem memiliki dua buah fungsional yaitu register akun dan ambil pasword. Fungsional register akun merupakan implementasi dari kebutuhan user untuk melakukan registrasi akun-akun yang akan dikelola dengan sistem perangkat lunak ini.



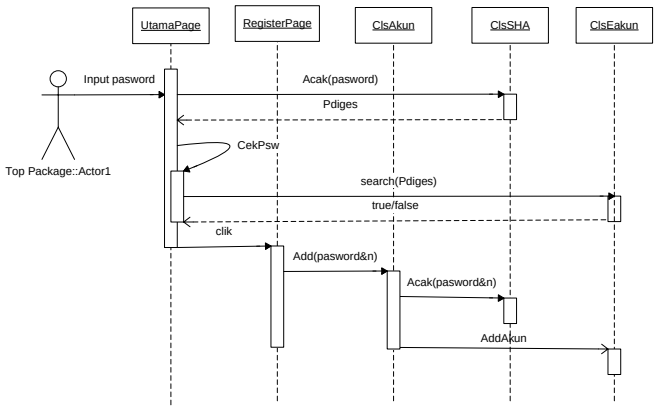
Gambar 3. Diagram usecase sistem

b) Perancangan Perangkat Lunak

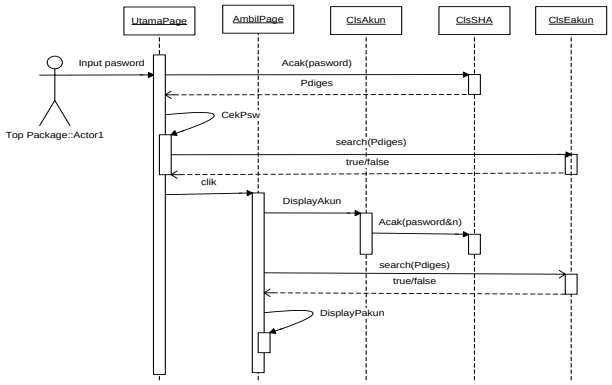
Perancangan kelas-kelas yang digunakan pada perangkat lunak terdapa pada tabel 5.1. Interaksi antar obyek pada perangkat lunak untuk setiap usecase dapat dilihat pada gambar 4 dan gambar 5.

Tabel 5.1. Daftar kelas

No	ama Kelas/Halaman	Keterangan
1	tamaPage	Halaman utama
2	egisterPage	Halaman interface registrasi akun
3	mbilPage	Halaman interface ambil pasword khusus
4	lsAkun	Kelas pengelola akun
5	lsSHA	Kelas fungsi SHA
6	lsEakun	Kelas entitas akun



Gambar 4 Diagram interaksi antar obyek register akun



Gambar 5. Diagram interaksi antar obyek register akun

c) Implementasi Perangkat Lunak

Kelas-kelas yang telah dirancang pada tahap sebelumnya telah diimplemantasikan kedalam beberapa kelas dengan bahasa PHP seperti terlihat pada tabel 5.1. Tabel tersebut mendeskripsikan adanya halaman web dan kelas yang berperan dalam perangkat lunak. Halaman dan kelas tersebut di dalam sistem perangkat lunak akan saling berinteraksi menghasilkan proses-proses yang menjadi mekanisme kerja fitur-fitur yang ada dalam usecase diagram.

d) Pengujian Perangkat Lunak

Hasil pengujian perangkat lunak disajikan pada tabel 5.2 dan 5.3.

Tabel 2. Tabel kasus uji register akun

No	Deskripsi	Masukan	Keluaran yang Diharapkan	Hasil yang Didapat	Kesimpulan
1	Tampilan Antar Muka register akun	-	Tampil halaman register akun	Tampil halaman register akun	Diterima

Tabel 3. Tabel kasus uji ambil pasword khusus

No	Deskripsi	Masukan	Keluaran yang Diharapkan	Hasil yang Didapat	Kesimpulan
1	Interface Form ambil akun	-	Halaman ambil akun	Halaman ambil akun	Diterima
2	Proses ambil akun	Klik tombol	Tampil pasword khusus	Tampil pasword khusus	Diterima

Berdasarkan hasil pengujian yang telah dilakukan pada tahap sebelumnya, dapat disimpulkan bahwa implementasi unit dan antar muka perangkat lunak berjalan dengan baik. Hal ini ditandai dengan kesimpulan hasil skenario pada kasus uji semuanya memberikan kesimpulan yang sama, yaitu diterima.

PENUTUP

A. Kesimpulan

Kesimpulan dari penelitian yang telah dilakukan adalah sebgai berikut:

a. Metode *common password* telah berhasil diimplementasikan pada sebuah perangkat lunak berbasis web..

b. Perangkat lunak implementasi metode pasword bersama dapat membantu pengguna dalam memudahkan pengelolaan berbagai pasangan akun dan pasword dengan cara menyalin (copy) pasword spesifik ke fasilitas login perangkat lunak yang dituju.

B. Saran

Perangkat lunak implementasi metode *common password* perlu dikembangkan lagi agar mampu melakukan koneksi secara otomatis ke perangkat lunak lain yang dibangkitkan passwordnya tanpa harus melalui login. Sehingga pengguna tidak lagi direpotkan dengan copy-paste password spesifik perangkat lunak yang dituju.

DAFTAR PUSTAKA

[1] Avestro,J. April, 2007. "*Pemgoraman Web*", Java Education Network Indonesia.

.[2] Luo Hui and Henry Paul. 2003. "*A Common Password Method for Protection of Multiple Accounts*", The 14th IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings

[3] Munir,R. 2006. "*Kriptografi*". Informarika. Bandung.

[4] Rhee Man Young, *Cryptography and Secure Communication*, McGraw-Hill, 1994

[5] Schneier, Bruce. 1996. "*Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C*". New York: John Wiley & Sons, Inc.

[6] Yong-Xia, Zhao. Ge, Zhen. 2010. "*MD5 research". IEEE International Conference on Multimedia and Information Technology*.

[7] Wali, M.F. and M. Rehan. "*Efective Coding and Performance Evaluation of the Rijndael Algorithm (AES)*". NED University of Engineering and Technology: Karachi, Pakistan