ANALISIS KEAMANAN PAIR BASED TEXT AUTHENTICATION PADA SKEMA LOGIN

Muhammad Munandar[1)], Arif Rahman Hakim[2)]
[1,2]Teknik Persandian, Sekolah Tinggi Sandi Negara
Jalan H. Usa Raya, Bogor, 16120
HP: +62 8572354 6377
E-mail : mohmoen93@gmail.com[1)]ArifHakim@stsn-nci.ac.id[2)]

Abstrak

Otentikasi pengguna merupakan proses pembuktian identitas pengguna dalam suatu sistem. Salah satu skema yang digunakan untuk otentikasi pengguna adalah skema login. Pada skema login, pengguna memberikan username dan password untuk membuktikan dirinya adalah pengguna yang sah. Password berbasis teks dan gambar terbukti rentan terhadap serangan yang ada, antara lain dictionary attack, brute force attack dan shoulder surfing. Pada makalah ini akan diuraikan metode alternatif dalam skema login, yaitu pair based text authentication. Fokus dari makalah ini adalah analisis keamanan pair based text authentication terhadap dictionary attack, brute force attack dan shoulder surfing. Selain itu, juga dibuat simulasi pair based text autentication dengan bahasa pemrograman PHP untuk memberikan gambaran jelas cara kerja pair based text sekaligus menggambarkan kemudahan penggunaan. Hasil penelitian yang diperoleh, pair based text authentication tahan terhadap serangan yang ada, yaitu dictionary attack, brute force attack dan shoulder surfing.

Kata kunci: *login, pair based text authentication, PHP.*

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Salah satu tujuan keamanan informasi adalah otentikasi entitas, yang disebut juga identifikasi. Otentikasi entitas merupakan pembuktian identitas suatu entitas (seseorang, komputer terminal, kartu kredit dan lain-lain). Salah satu contoh otentikasi entitas adalah otentikasi pengguna (*user authentication*), yaitu seorang pengguna harus membuktikan identitasnya sebagai pengguna yang sah untuk dapat masuk ke dalam sistem.

Salah satu skema yang digunakan untuk otentikasi pengguna adalah skema *login*. Pada skema *login*,pengguna memberikan identitas berupa *username* dan *password* untuk membuktikan dirinya adalah pengguna yang sah. Sistem melakukan verifikasi kesesuaian identitas dari pengguna dengan daftar identitas sah yang dimilikinya. Jika verifikasi berhasil, pengguna dapat masuk dan mengakses layanan tertentu yang ada dalam sistem. Jika verifikasi gagal, pengguna tidak dapat masuk ke dalam sistem dan diminta untuk memberikan kembali identitas yang benar. Asumsi dalam skema ini adalah identitas yang sah hanya diketahui dan digunakan oleh pengguna yang bersesuaian dengan identitas sah tersebut. Dengan demikian setiap pengguna yang masuk ke dalam sistem terjamin keasliannya (otentik).

Password yang digunakan pada skema *login* dapat berbasis teks (*textual password*) atau berbasis gambar (*graphical password*). *Password* berbasis teksrentan terhadap upaya *dictionary attack*, *bruteforce attack* dan *shoulder surfing.* Sedangkan *password* berbasis gambarmembutuhkan sumber daya yang lebih besar dan waktu proses yang lebih lambat. Selain itu, *password* berbasis gambarrentan terhadap *shoulder surfing.* Oleh karena itu, perlu dilakukan analisis keamanan metode autentikasi alternatif pada skema *login* yang tahan terhadap serangan (*attack*) yang ada dan tetap mudah digunakan oleh pengguna.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah tersebut, maka rumusan masalah difokuskan pada:

1) Bagaimana analisis keamanan *pair based text authentication* pada skema *login* terhadap upaya *dictionary attack*, *brute force attack* dan *shoulder surfing*?
2) Bagaimana analisis perbandingan tingkat keamanan *pair based text authentication* dibandingkan metode *password* berbasis teks dan *password* berbasis gambar?

Analisis keamanan terhadap serangan tidak dilakukan secara empiris, hanya berdasarkan tingkat kesulitan atau kompleksitas serangan tersebut untuk mendapatkan *password* yang tepat dari banyaknya kemungkinan *password* yang dicoba.

1.3 Tujuan

Tujuan penulisan ini adalah sebagai berikut :

1) Menganalisis keamanan metode *pair based text authentication* pada skema *login* terhadap upaya *dictionary attack, brute-force attack* dan *shoulder surfing*.
2) Menganalisis perbandingan *password* berbasis teks, *password* berbasis gambardan *pair based text authentication* terhadap upaya *dictionary attack, brute-force attack* dan *shoulder surfing.*

2. LANDASAN TEORI

2.1 Otentikasi Pengguna

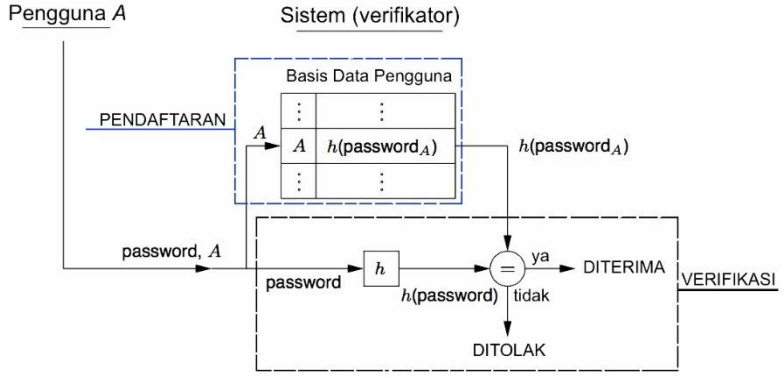
Otentikasi pengguna merupakan bagian dari otentikasi entitas atau identifikasi, yaitu pembuktian terhadap identitas suatu entitas, bisa berupa orang, kartu kredit atau mesin[5]. Teknik ini merupakan proses dimana satu pihak dapat menjamin atau memastikan pihak kedua terlibat langsung. Terdapat tiga basis pada teknik identifikasi[2], yaitu:

1) Sesuatu yang diketahui (*something known*), yaitu identifikasi berdasarkan pada sesuatu yang diketahui dan dapat diingat. Seperti *password* dan *Personal Identification Number* (PIN).
2) Sesuatu yang dimiliki (*something possesed*), yaitu identifikasi berdasarkan pada sesuatu yang dimiliki. Contohnya seperti token dan *smartcard*.
3) Sesuatu yang melekat (*something inherent*), yaitu identifikasi dengan menggunakan bagian unik anggota tubuh, berupa sidik jari, iris mata, dan bagian tubuh unik lainnya. Proses ini tidak menggunakan kriptografi secara langsung.

2.2 Skema *Login*

Login merupakan skema identifikasi pengguna melalui pembuktian identitas berupa *username* dan *password*. Secara umum skema *login* terbagi menjadi dua fase, yaitu:

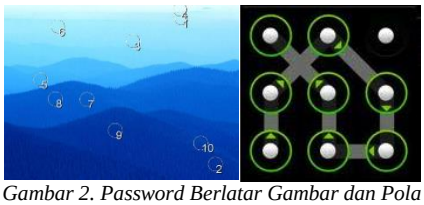
1) Registrasi, yaitu pendaftaran pengguna dalam sistem. Pengguna memberikan *username* dan *password* kepada sistem. Sistem menyimpan *username* dan nilai hash *password* ke dalam basis data (*database*) pengguna.
2) Verifikasi, yaitu pengecekan pengguna yang sah untuk mengakses sistem. Pengguna memasukkan *username* dan *password* yang telah didaftarkan sebelumnya. Sistem menghitung nilai *hash* dari *password* yang dimasukkan dan mencocokkan nilai *hash* tersebut dengan nilai *hash password* yang tersimpan dalam basis data sesuai *username.* Jika sesuai, maka pengguna diijinkan mengakses sistem, sebaliknya, pengguna tidak dapat mengakses sistem dan kembali diminta untuk memasukkan *username* dan *password* yang benar.



Gambar 1. Pendaftaran dan Verifikasi pada Skema Login

Password digunakan sistem untuk memastikan seseorang sebagai pengguna yang sah. *Password* terdiri dari dua jenis berdasarkan bentuk yang digunakan, yaitu:

1) *Password* berbasis teks, merupakan metode otentikasi pengguna dengan menggunakan rangkaian karakter berupa huruf, angka, dan simbol[1]. Contohnya, PIN kartu ATM, *password* surel dan media sosial.
2) *Password* berbasis gambar, merupakan metode yang digunakan untuk otentikasi pengguna menggunakan media gambar. Berdasarkan tipe latar gambar yang digunakan, *password* berbasis gambar terbagi menjadi dua jenis yaitu[1]:
   a. Password dengan latar gambar. Pengguna diminta untuk mengenali gambar yang dipilih pada fase pendaftaran.
   b. Password berlatar pola (*grid*). Pengguna diminta untuk mengkonstruksi pola seperti pola yang ditentukan pada fase pendaftaran.



Gambar 2. Password Berlatar Gambar dan Pola

2.3 Serangan pada Skema *Login*

Serangan adalah upaya kriptanalisis yang dilakukan dengan cara mengeksploitasi kelemahan dari suatu algoritma maupun protokol kriptografi[5]. Beberapa jenis serangan pada *password* yang banyak digunakan antara lain :

1) *Dictionary attack*, merupakan serangan dengan mencoba menebak kata atau rangkaian karakter yang biasa atau sering digunakan sebagai *password*. Seperti tanggal lahir, nama orang tua, nomor telepon, dan lainnya
2) *Brute force attack*, merupakan serangan dengan mencoba semua kemungkinan dengan mencoba berbagai kombinasi karakter satu per satu hingga *password* yang sebenarnya ditemukan. Misalnya dengan mencoba kombinasi PIN angka 4 digit mulai 0000, 0001, 0002, 0003, dan seterusnya hingga kombinasi 9999
3) *Shoulder surfing*, merupakan serangan dengan mengamati secara langsung ketika pengguna memasukan *password*[7]. Misalnya dengan menggunakan bantuan alat seperti kamera tersembunyi ataupun aplikasi seperti *key loger*.

Pada *password* berbasis teks, *password* yang digunakan harus dibuat sesulit mungkin untuk ditebak. Penggunaan *password* yang sederhana dan mudah ditebak (seperti tanggal lahir, nama, nomor ponsel, dan lain-lain) akan meningkatkan kerawanan terhadap *dictionary attack, brute force attack*, dan *shoulder surfing*. *Dictionary attack* pada *password* berbasis gambar tidak dapat dilakukan karena tidak ada kamus gambar yang dapat digunakan, atau tidak dapat menebak suatu gambar yang sering digunakan. Namun, *brute force attack* masih mungkin dilakukan dengan mencoba seluruh gambar yang bisa dipilih atau seluruh pola yang dapat dibentuk. Kecuali itu, *password* berbasis gambar sangat rentan terhadap *shoulder surfing*.

Tabel 1. Serangan pada *Password* Berbasis Teks *dan Password* Berbasis Gambar[3]

Serangan	*Password* Berbasis Teks	*Password* Berbasis Gambar
Dictionary Attack	√√√	√
Brute Force Attack	√√	√√
Shoulder Surfing	√√√	√√√

Ket: √√√=sangat mudah √√=mudah √=sulit

3. OTENTIKASI PENGGUNA DENGAN *PAIR BASED TEXT AUTHENTICATION LOGIN*

Proses otentikasi pengguna ini secara garis besar terbagi menjadi 3 fase[4], yaitu:

1) Proses registrasi, pengguna mendaftarkan *username* dan *password* yang akan digunakan. Setelah itu, sistem akan menyimpan data tersebut pada *database*.
2) Proses *login*, yaitu proses untuk masuk ke sistem setelah pengguna melakukan registrasi. Pada prosesnya, sistem akan mengirimkan skema *pair based textauthentication* untuk menghasilkan *session password* yang dibuat oleh pengguna dengan mengacu pada *password* miliknya. *Pair based text authentication* tersebut berupa matriks berisi karakter huruf, angka dan simbol yang berubah setiap kali pengguna *login*. Sehingga setiap kali *login* pengguna memasukan *password* yang berbeda.
3) Proses verifikasi, proses ini berlangsung pada sistem, yaitu sistem menverifikasi data (*username* dan *sessionpassword*) yang diinputkan oleh pengguna. Jika data tersebut sesuai maka pengguna diijinkan masuk sistem, sebaliknya pengguna tidak mengizinkan masuk ke sistem dan diminta untuk memasukkan data yang benar.

Karakteristik skema ini adalah penggunaan *pair based text authentication* (berupa matriks) pada proses *login*, sehingga pengguna menggunakan *password* yang berbeda setiap kali melakukan *login*. Berikut adalah contoh gambar matriks yang diberikan sistem.

<	?	7	M	[	}	6	/
Q	>	J	{	K	Y	`	T
1	(	)	2	_	+	U	~
*	W	8	-	L	;	‘	N
G	^	H	E	]	3	R	4
&	F	9	O	Z	P	I	:
.	%	0	C	!	@	V	B
,	D	S	$	X	A	#	5

Gambar 3. Contoh Matriks Pair Based Text

Misalnya, *password* pengguna adalah 4kU, maka ketika *login* pengguna tidak menuliskan *password* tersebut secara langsung. Tapi, menggunakan matriks yang telah disediakan sistem, pengguna memilih pasangan karakter yang membentuk *password* yang dimilikinya. Karakter pertama mewakili baris dan karakter kedua mewakili kolom pada matriks. Perpotongan baris dan kolom tersebut menunjukkan karakter *password* pengguna.

<	?	7	M	[	}	6	/
Q	>	J	{	K	Y	`	I
1	(	)	2	_	+	U	~
*	W	8	-	L	;	‘	N
G	^	H	E	]	3	R	4
&	F	9	O	Z	P	I	:
.	%	0	C	!	@	V	B
,	D	S	$	X	A	#	5

Gambar 4. Kombinasi Pasangan Karakter HT Membentuk Karakter Password 4

Pengguna dapat memilih berbagai macam kombinasi karakter dari baris dan kolom yang membentuk *password* miliknya. Pilihan untuk karakter 4 antara lain]N atau HT atau HN atau pasangan karakter lainnya. Dan seterusnya, begitupun dengan karakter *password* lainnya menggunakan cara yang sama.

4. SIMULASI METODE *PAIR BASED TEXT AUTHENTICATION LOGIN* DENGAN BAHASA PEMROGRAMAN PHP

Bahasa pemrograman PHP merupakan bahasa pemrograman yang berbasis *web*. Oleh karena itu, PHP digunakan untuk simulasi *pair based text authentication* sebagai metode *login* pada aplikasi web. Simulasi yang dibuat juga menggunakan *database* untuk menyimpan seluruh data pengguna. Simulasi yang dibuat bertujuan untuk menggambarkan cara kerja *pair based text authentication* dan mengambarkan kemudahan penggunaan bagi pengguna untuk masuk sistem. Simulasi yang dibuat diasumsikan aman dari kerawanan bahasa pemrograman *web* seperti *sidejacking*, *http post* dan lain-lain,sehingga simulasi ini tidak menggambarkan keamanan dari kerawanan bahasa pemrograman *web* dan keamanan *server* yang digunakan. Berikut penjelasan singkat simulasi yang dibuat:

1) Pada halaman awal, pengguna akan dihadapkan dengan pilihan, yaitu MASUK dan DAFTAR. MASUK dipilih/diklik jika pengguna belum terdaftar pada sistem. Sementara MASUK digunakan bagi pengguna yang sudah terdaftar dan akan masuk ke sistem.
2) Jika pengguna belum terdaftar, maka pilih/klik DAFTAR. Kemudian pengguna harus memasukan data berupa *username* yang akan digunakan setiap kali *login* dan *password* sebagai acuan *session password* setiap kali *login*.
3) Setelah melakukan pendaftaran/registrasi. Pengguna dapat masuk ke sistem melalui proses *pair based text authentication*, dengan *password* terdaftar dijadikan acuan untuk melakukan *login*.

Pengguna dapat memilih kombinasi pasangan karakter dari matriks yang telah tersedia. Dari pasangan karakter tersebut nantinya membentuk *password* milik pengguna. Setelah selesai, pengguna pilih/klik MASUK. Jika data yang dimasukan benar maka pengguna bisa masuk, jika salah maka permohonan *login* ditolak.

Berikut tangkapan (*capture*) gambar simulasi *login* menggunakan *pair based text authentication*:

Gambar 5. Halaman Awal

Gambar 6. Halaman Registrasi

Gambar 7. Halaman Login

Gambar 8. Halaman Berhasil Login

Gambar 9. Halaman Gagal Login

5. ANALISIS SERANGAN PADA PENERAPAN *PAIR BASED TEXT AUTHENTICATION*

Skema *login* dengan *pair based text authentication* berdasarkan serangan yang ada dapat dianalisis sebagai berikut:

1) *Session* yang dihasilkan oleh matriks *pair based text authentication* bersifat acak dan hanya digunakan satu kali setiap kali *login*membuat upaya *dictionary attack* sulit dilakukan.
2) Matriks yang dinamis (berubah setiap kali *login*) membuat upaya *bruteforce attack* pada metode *pair based text authentication* sulit dilakukan.
   Penggunaan matriks ini sangat berbeda dengan CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) yang banyak digunakan pada situs untuk membedakan komputer dan manusia untuk mencegah *spammer*. Pada CAPTCHA, pengguna diminta untuk menuliskan karakter (kode) yang terkandung dalam sebuah gambar, yang sangat mudah dibaca oleh manusia namun sulit dibaca oleh komputer. Namun saat ini terdapat teknik yang dapat digunakan untuk menembus CAPTCHA yaitu teknik OCR (*Optical Character Recognition*). OCR memungkinkan komputer untuk mengkonversi gambar CAPTCHA menjadi teks, sehingga komputer dapat mengenali teks tersebut dan menembus ujian CAPTCHA. Berbeda dengan CAPTCHA, pada matriks *pair based text authentication*, pengguna yang ingin masuk sistem tidak menuliskan seluruh karakter yang ada dalam matriks, namun hanya pasangan-pasangan karakter yang terkait dengan *password* yang dimiliki. Pengguna yang tidak mengetahui *password* yang benar, tidak akan mampu mengisi pasangan karakter (*session password*) meskipun ia dapat membaca seluruh karakter yang ada dalam matriks. Oleh karena itu, teknik OCR yang sering digunakan untuk menembus CAPTCHA tidak dapat digunakan pada skema *pair based text authentication* tanpa mengetahui *password* yang benar.
3) *Session* yang acak dan sekali pakai serta matriks yang dinamis membuat upaya *shoulder surfing* sulit dilakukan. *Shoulder surfing* harus dilakukan berulang kali terhadap pengguna yang sama untuk mencocokkan baris dan kolom yang bersesuaian, sehingga mendapatkan karakter *password* pengguna yang tepat.

Perbandingan keamanana *password* berbasis teks, *password* berbasis gambardan *pair based text authentication* terhadap upaya *dictionary attack, bruteforce attack* dan *shoulder surfing* dapat dilihat pada tabel berikut:

Tabel 2. Perbandingan Keamanan *Password* Berbasis Teks, *Password* Berbasis Gambardan *Pair Based Text Authentication*

Serangan	*Password* Berbasis Teks	*Password* Berbasis Gambar	*Pair Based Text Authentication*
Dictionary Attack	√√	√	√
Brute Force Attack	√√	√√	√
Shoulder Surfing	√√√	√√√	√

Ket: √√√=sangat mudah √√=mudah √=sulit

6. SIMPULAN DAN SARAN

6.1 Simpulan

Kesimpulan dari hasil penelitian ini adalah sebagai berikut:

1) Metode *pair based text authentication* pada skema *login*sulit untuk dilakukan serangan dengan *dictionary attack, brute-force attack* dan *shoulder surfing.*
2) Metode *pair based text authentication* memiliki tingkat keamanan yang lebih baik dibandingkan metode *password* berbasis teksdan *password* berbasis gambar ditunjau dari upaya *dictionary attack, brute-force attack* dan *shoulder surfing.*

6.2 Saran

Adapaun saran penulis untuk pengembangan penelitian adalah sebagai berikut:

1) Perlu dilakukan perbandingan kinerja berdasarkan kompleksitas data, memori dan waktu dari metode *password* berbasis teks, *password* berbasis gambar dan *pair based text authentication.*
2) Perlu dilakukan penelitian perbandingan tingkat keamanan *pair based text authentication* dengan metode identifikasi dua faktor atau lebih.

7. DAFTAR RUJUKAN

[1] Menezes, A., Oorschot, P., dan Vanstone, S., 1996. *Handbook of Applied Cryptography*. CRC Press.

[2] Tim Penyusun Lembaga Sandi Negara., 2007. *Jelajah Kriptologi*. Jakarta: Lembaga Sandi Negara.

[3] Hidayat, R., Virgono, A., dan Usman , K., 2010. *Desain dan Implementasi Sistem Autentikasi dengan Graphical Password Berbasis Pixel Selection*. Konferensi Nasional Sistem dan Informatika, KNS&I10-032**.**

[4] Sabzevar, A. dan Stavrou, A. *Universal Multi-Factor Authentication Using Graphical Passwords.*George Mason University, Fairfax, Virginia, 22030.

[5] Sreelatha, M., Shashi, M., dan Anirudh, M., 2011. *Authentication Schemes for Session Passwords using Color and Images*. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3.

[6] Pengertian *Password*, http://en.wikipedia.org/wiki/Password, diakses terakhir tanggal 1 Juni 2013.

[7] Pengertian *Shoulder Surfing*, http://id.wikipedia.org/wiki/Shoulder_Surfing, diakses terakhir tanggal 1 Juni 2013.