ANALISIS CUED RECALL GRAPHICAL PASSWORD SYSTEM RESISTANT TO SHOULDER SURFING (CRGPS) DALAM PERMASALAHAN SHOULDER SURFING ATTACK PADA AUTHENTICATION

Angger Mahastyo L[1], Tjokorda Agung Budi Wirayuda[2], Vera Suryani[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Cued Recall Graphical Password System Resistant to Shoulder Surfing (CRGPS) adalah salah satu skema graphical password yang menggunakan gambar sebagai cued yang membantu user pada saat pengisian password. Kelebihan dari graphical password yaitu mempermudah user dalam mengingat password melalui gambar-gambar yang disediakan dan kombinasi password yang sangat besar. Tetapi terdapat kelemahan pada graphical password terhadap serangan shoulder surfing yang masih menjadi kendala. CRGPS diajukan dengan tujuan mampu menahan serangan shoulder surfing dengan menggunakan gambar sebagai cued.

Tetapi karena CRGPS menggunakan textual password lebih dari satu, perlu diketahui berapa minimal karakter yang dapat digunakan tanpa mengurangi keamanan sistem ini terhadap shoulder surfing attack. Dengan menguji sistem CRGPS yang menggunakan 6 sampai 4 panjang karakter pada textual password terhadap 10 partisipan yang berperan sebagai penyerang yang menggunakan shoulder surfing attack, dapat memperlihatkan bahwa sistem ini mampu menahan serangan shoulder surfing walau dengan panjang karakter yang sedikit. Selain itu akan dilakukan pengujian dengan menggunakan keylogger dan kemudian menganalisis hasilnya untuk melakukan penyerangan terhadap sistem. Untuk membangun sistem CRGPS akan digunakan script PHP yang terdapat pada software XAMPP 1.7.3. Hasil menunjukkan CRGPS mampu menahan serangan shoulder surfing hingga 100%, tapi masih lemah menghadapi serangan keylogger sederhana yang memonitor setiap login user dan kemudian menggunakannya untuk menyerang sistem.

Kata Kunci : autentikasi, graphical password, shoulder surfing, textual password

---

Abstract

Cued Recall Graphical Password System Resistant to Shoulder Surfing (CRGPS) is one of the graphical password schemes that use the images as cued which helps the user at the time filling the passwords. The advantages of graphical passwords are easier for users to remember the password through the picture provided and the passwords combination is very large. Therefore, the password is quite difficult to penetrate with brute force attacks. But the weakness of graphical password is till in constraint. CRGPS proposed with the aim of shoulder surfing able to withstand attacks by using images as cued.

But because CRGPS use textual password more than one time, to fill the password we need to find out how minimum of character that can be used without compromising the system's security against shoulder surfing attacks. By testing CRGP system that uses 6 to 4 characters long on textual password against 10 participants who plays as shoulder surfing attackers, could show that the system is able to withstand the attack of shoulder surfing even though the characters are short. Additionally, it will be tested by using a keylogger and then analyze the results which is use to attacks the system. To build CRGPS system we will be using PHP script which is contained on XAMPP 1.7.3. The results showed CRGPS able to withstand shoulder surfing attacks up to 100%, but still weak against simple keylogger attacks that monitors each user's login and then use it to attack the system

Keywords : authentication, graphical password, shoulder surfing, textual password

---

1. Pendahuluan

1.1 Latar Belakang

Autentikasi (authentication) merupakan suatu proses untuk mengetahui, memeriksa memastikan suatu kebenaran bahwa user yang mengaku terhadap suatu identitas adalah user yang sebenarnya. Seperti saat kita melakukan login pada suatu website, kita diharuskan untuk memasukkan data diri kita berupa username dan string rahasia berupa password. Namun tidak sedikit pengguna autentikasi mengalami kesulitan untuk mengingat kombinasi huruf-angka (alphanumeric) tersebut. Untuk mengatasi masalah ini, akhirnya user cenderung menggunakan password yang lemah seperti penggunaan kata dalam kamus atau terkait data pribadi (personal information) sehingga permasalahan keamanan muncul dan password menjadi riskan diketahui [12].

Untuk mengatasi permasalahan ini dikembangkan alternatif autentikasi lain disamping alphanumeric password (*textual password*). Berdasarkan sebuah hipotesa bahwa manusia lebih baik dalam mengingat gambar daripada kata-kata. Fakta yang didapat, kemampuan manusia untuk mengingat (*recalling*) jauh di bawah kemampuan untuk mengenali (*recognition*) [15]. Berdasarkan hal ini dikembangkan autentikasi graphical password.

Graphical password adalah sistem keamanan menggunakan password dengan menggunakan bantuan gambar (*picture*) atau menggunakan gambar tersebut sebagai bentuk password. Graphical password dikembangkan untuk mengatasi kekurangan pada alphanumeric password. Pada graphical password, proses autentikasi dilakukan dengan menggunakan bantuan atau pemilihan gambar sehingga kita dapat meminimkan proses recalling dalam autentikasi. Penyerang dapat berdiri di belakang pengguna dan secara langsung mengamati monitor atau mencoba dari jarak yang tidak terlalu jauh agar tidak dicurigai dan kemudian mengamati gerakan tangan atau ketikkan user pada keyboard.

Cued Recall Graphical Password System Resistant to Shoulder Surfing (CRGPS) adalah salah satu skema *cued recall based system* pada graphical password yang mencoba untuk mengatasi shoulder surfing [6]. CRGPS menggunakan gambar-gambar sebagai pengingat password kita dimana masing-masing gambar dapat mewakili satu buah password yang dapat diasosiasikan dengan gambar tersebut. Gambar-gambar yang dijadikan sebagai bagian password diselipkan diantara sejumlah gambar lainnya untuk mempersulit penyerang. Dan setiap proses autentikasi dimulai, gambar-gambar yang muncul selalu berbeda dan acak. Bila penyerang gagal memasukkan password yang benar sebanyak tiga kali, maka penyerang akan dikeluarkan dari proses autentikasi

Dalam tugas akhir ini, akan dilakukan analisis kemampuan CRGPS terhadap serangan shoulder surfing pada autentikasi yang dilakukan sesuai dengan skenario shoulder surfing yang dibuat dan kemudian menghitung keberhasilan penyerang masuk ke dalam sistem. Persentase keberhasilan dan kegagalan penyerang masuk ke dalam sistem akan menjadi parameter dari ketahanan CRGPS. Dengan diimplementasikan nya CRGPS diharapkan dapat menahan serangan shoulder surfing yang masih menjadi kendala bagi skema graphical password yang sebelumnya.

1.2 Perumusan Masalah

Seperti yang telah disebutkan sebelumnya bahwa permasalahan yang dihadapi adalah skema graphical password terdahulu masih mengalami permasalahan terhadap serangan shoulder surfing. Untuk itu dirancang sebuah sistem CRGPS yang merupakan web based system. Karena pada sistem CRGPS juga terdapat 4 textual password, perlu diketahui berapa minimal panjang karakter yang diperlukan tanpa mengurangi keamanan dari sistem CRGPS tersebut.

1. Bagaimana mengimplementasikan sistem CRGPS ke dalam bentuk web based system.
2. Berapa minimal panjang karakter yang diperlukan di setiap textual password yang terdapat pada sistem tapi sistem masih mampu menahan serangan shoulder surfing.
3. Bagaimana kemampuan CRGPS terhadap keylogger sederhana.

1.3 Batasan Masalah

Agar pengerjaan tugas akhir ini tidak keluar jalur dari perumusan masalah yang ingin dicapai, perumusan masalah pada tugas akhir ini berada pada skenario shoulder surfing yang berarti serangan yang digunakan hanya shoulder surfing dan juga penyerangan menggunakan keylogger sederhana. Pada skenario shoulder surfing, partisipan yang berperan sebagai penyerang mengamati secara langsung tanpa alat hardware atau software saat user melakukan autentikasi. 150 gambar yang berfungsi sebagai *cued* atau pengingat telah disediakan dan dikategorikan ke dalam lima kategori, yaitu Hewan, Permainan dan Olahraga, Kendaraan dan Transportasi, Peralatan Umum, dan Rambu-rambu yang kemudian akan dilakukan survey untuk mendapatkan 125 gambar yang dipilih terbanyak yang kemudian akan digunakan di dalam sistem. Bila terdapat jumlah pilihan survey yang sama banyak, penulis dapat memilih gambar mana yang akan dimasukkan ke dalam sistem. Diasumsikan bahwa proses Registrasi (*register*) dan Reset terjadi dengan aman.

1.4 Tujuan

Tujuan dari penulisan tugas akhir ini, yaitu:

1. Membangun skema graphical password yaitu Cued Recall Graphical Password System Resistant to Shoulder Surfing (CRGPS).
2. Membangun CRGPS yang mampu menahan serangan shoulder surfing sesuai skenario shoulder surfing yang telah ditentukan.
3. Mengetahui berapa minimal panjang karakter yang diperlukan di setiap textual password yang terdapat pada sistem tapi sistem masih mampu menahan serangan shoulder surfing
4. Mengetahui ketahanan CRGPS terhadap keylogger sederhana.

.

1.5 Metodologi Penyelesaian Masalah

1. Studi Literatur
   Pada tahap studi literatur akan dilakukan pendalaman materi mengenai graphical password dan skem-skema yang telah ada sebelumnya. Memahami lebih jauh kekurangan dan kelebihan skema graphical password yang ada sebelumnya dalam proses autentikasi.
2. Analisis Permasalahan dan Perancangan Sistem
   Pada tahap analisis permasalahan akan menganalisis permasalahan graphical password terhadap shoulder surfing dalam proses autentikasi. Dan kemudian merancang pembangunan sistem CRGPS. Pada saat perancangan sistem akan dilakukan juga perancangan password. Dalam sistem CRGPS password yang digunakan adalah textual password (pass_code) yang menggunakan gambar (pass_object) sebagai bagian dari graphical password yang berfungsi sebagai cued. Jumlah gambar yang digunakan ada 125 gambar yang dikelompokkan ke dalam 5 kategori (Hewan, Kendaraan dan Transportasi, Permainan dan Olahraga, Peralatan Umum dan Rambu-rambu). Dengan mengelompokkan gambar-gambar tersebut diharapkan dapat mempermudah proses recall yang dilakukan user.
3. Implementasi
   Melalui rancangan sistem yang telah dibuat sebelumnya, akan diimplementasikan ke dalam sistem CRGPS. Hasil survey untuk mendapatkan 125 gambar akan digunakan dalam sistem CRGPS. Dalam 125 gambar tersebut, user akan memilih 5 gambar yang akan dijadikan pass_object dan berasosiasi dengan pass_code yang user pilih sendiri.
4. Pengujian dan Analisis Hasil
   Pengujian dilakukan untuk mengetahui ketahanan sistem CRGPS terhadap serangan shoulder surfing dan mengetahui penggunaan minimal password yang diperlukan agar sistem masih dapat dikatakan aman. Hasil gambar yang dipilih melalui survey akan menjadi bagian sistem CRGPS dan diujikan untuk mengetahui ketahanan CRGPS terhadap serangan shoulder surfing sesuai skenario shoulder surfing dan pada saat itu juga diujikan untuk mengetahui penggunaan minimal password dengan mengubah panjang password sedikit demi sedikit, selama penyerang masih belum mampu menembus sistem dan selama batas kewajaran.
5. Pembuatan Laporan
   Pada tahap ini penyusunan laporan akan dilakukan untuk mendokumentasikan pendeskripsian masalah serta hasil yang diperoleh sampai selesai.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil implementasi, pengujian dan analisis yang telah dilakukan sebelum nya yang bertujuan untuk memeriksa ketahanan sistem CRGPS terhadap serangan shoulder surfing dengan menggunakan panjang karakter yang telah diujikan dan menggunakan keylogger sederhana, dapat diambil kesimpulan sebagai berikut :

1. CRGPS merupakan skema graphical password yang dapat menahan serangan shoulder surfing dengan baik dalam kondisi penyerang tidak menggunakan hardware atau software tertentu sesuai dengan pengujian.
2. Semakin panjang password tentu akan semakin baik dalam proses autentikasi. Sementara hal tersebut berbanding terbalik dengan keinginan user dimana semakin pendek password, semakin mudah juga user dapat mengingatnya dan password yang panjang akan menyulitkan user untuk mengingat password apa yang digunakan. CRGPS menggunakan 5 textual password, dimana 3 diantaranya akan muncul pada saat login. Secara total, tentu CRGPS memiliki password yang sangat panjang. Walau demikian, CRGPS menggunakan gambar untuk mengingatkan user, password apa yang digunakan. Lalu untuk membantu user lebih jauh, perlu diketahui berapa minimal panjang password untuk setiap pass code tapi sistem masih tetap aman. Hasil menunjukan bahwa walau dengan menggunakan 4 panjang karakter yang dimasukan pada pass code, sistem masih aman.
3. Sistem CRGPS tidak sepenuhnya mampu menahan serangan keylogger sederhana. Bila penggunaan keylogger digunakan untuk memonitor setiap sesi login user, maka pass_code bisa saja didapatkan dengan menganalisa hasil monitor keylogger. Oleh karena itu fake pass_code menjadi hal yang penting untuk menyulitkan penyerang mendapatkan seluruh pass_code milik user walau fake pass-code tidak menambah kombinasi urutan pass-code secara matematis.

5.2 Saran

Saran untuk pengembangan tahap selanjutnya adalah :

1. Agar lebih memperhatikan gambar yang akan digunakan untuk graphical password. Gambar ini merupakan hal yang penting dalam graphical password, khususnya CRGPS yang menggunakan gambar

tersebut sebagai *cued*. Gambar tersebut harus cukup jelas bagi pengguna yang memakai sistem CRGPS. Oleh karena itu ukuran gambar perlu diperbesar.

2. Menggunakan layar monitor yg juga cukup besar untuk menghindari user menggunakan mouse untuk scroll gambar pada saat mengamati gambar untuk menemukan pass_object nya. Hal ini perlu dilakukan agar penyerang tidak melihat user fokus pada bagian gambar tertentu.
3. Kelemahan graphical password pada umunya juga terletak pada waktu login yang terlampau jauh jika dibandingkan dengan textual password. Diharapkan ada solusi untuk memperpendek waktu tersebut dan tidak mengorbankan keamanan yang baik dari sistem ini.
4. Pengujian performansi sistem akan dapat membantu membandingkan bagaimana sistem CRGPS menggunakan resources dibandingkan dengan tradisional password pada umumnya.

Daftar Pustaka

[1] A. Adams, M. Sasse, and P. Lunt. Making Passwords Secure and Usable. People and Computers XII, pages 1–20, 1997

[2] D. Davis, F. Monrose, and M. K. Reiter, "OnUser Choice in Graphical Password Schemes," Proceedings of the 13th USENIX Security Symposium (Aug. 2004).

[3] D. Gollman. Computer security. John Wiley and Sons Ltd, 1999.

[4] D. Norman. The Design of Everyday Things. Basic Books, 1988.

[5] F.Tari, A.A Ozok, S.H. Holden. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords

[6] Hooi li Lai,. Cued Recall Graphical Password System Resistance to Shoulder Surfing. Thesis, 2009

[7] James S. Nairne, Josefa N.S.P "Adaptive Memory : Is Survival Processing Special?", Journal of Memory and Languange, 2008

[8] L. Standing. Learning 10,000 pictures. Quarterly journal of Experimental, pages 207–222, 1973.

[9] L. Standing, J. Conezio, and R. Haber. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. Psychonomic Science, pages 73–74, 1970

[10] M. Backes, M. Drmuth, and D. Unruh. Compromising Reflections - or - How to Read LCD Monitors Around the Corner. In IEEE Symposium on Security and Privacy, May 2008

[11] Picking and Protecting Passwords, University of Miami Ethics Programs

[12] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memory. "Authentication using graphical passwords: Basic Results", Proc. Human-Computer Interaction International (2005)

[13] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memory. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice.

[14]Shepard, R.N. Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior 6

[15] Wixted, T.J. The psychology and neuroscience of forgetting. Annual Review of Psychology 55 (2004).

Telkom University