OTENTIKASI MULTI FAKTOR UNTUK MENINGKATKAN KEAMANAN KOMPUTER

M.RUDYANTO ARIEF[1]

Abstract

In today's networked, Internet-enabled world of e-Commerce, e-Business and e-Government, ensuring that only legitimate, authenticated individuals can access your organization's IT resources is vital. Without proper authentication, other security systems (for example, a firewall or VPN) provide little or no protection against intruders, because an intruder can masquerade as a legitimate user and access any resource that the latter person could.

Keywords

username, password, brute force attack, social engineering, intruder, authentication, biometrics, voice recognation.

Pendahuluan

Perkembangan internet saat ini sudah semakin pesat. Dengan munculnya e-Commerce, e-Bussiness, e-Government maka masalah keamanan data atau informasi merupakan suatu keharusan. Artinya hanya user yang sah, orang yang memiliki hak akses yang boleh mengakses sumber daya yang ada di sebuah organisasi. Tanpa menggunakan metode otentikasi yang tepat maka penggunaan metode keamanan sistem keamanan yang lain seperti VPN atau Firewall menjadi tidak berarti apapun. Sistem keamanan ini hanya menyediakan sedikit pengamanan pada sebuah sistem dari adanya pengacau (intruder) yang mencoba untuk mengakses sistem kita. Karena pengacau dapat saja menyamar sebagai seorang user yang sah dan dapat mengakses semua sumber daya yang ada dalam sebuah organisasi.

[1] JURUSAN TEKNIK INFORMATIKA
STMIK AMIKOM YOGYAKARTA

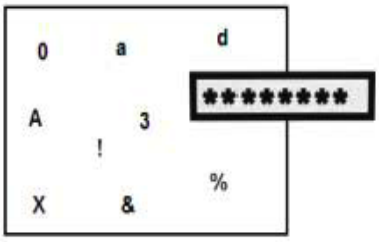
Otentikasi merupakan sebuah mekanisme yang di gunakan untuk melakukan validasi terhadap identitas user yang mencoba mengakses sumber daya dalam sebuah sistem komputer. Metode otentikasi konvensional yang selama ini familiar di gunakan adalah menggunakan kombinasi “username” dan “password” atau biasa juga di sebut dengan metode “single factor authentication”. Username adalah sebuah penanda unik yang dapat digunakan untuk mengidentifikasi seorang user yang mencoba masuk (log on) kedalam sebuah sistem komputer. Password adalah sebuah kombinasi rahasia yang terdiri dari kombinasi huruf, angka, dan karakter khusus. Username dan password di kombinasikan bersama-sama untuk mekanisme otentikasi pada sebuah sistem komputer.

Gambar 1 Kombinasi username dan password

Ketika username dan password seseorang sudah di ketahui oleh penyerang maka tidak ada mekanisme berikutnya yang dapat menghalangi akses yang di lakukan oleh seorang penyerang terhadap sistem dalam sebuah organisasi. Mengapa kombinasi username dan password ini rentan terhadap serangan oleh pengacau? Hal ini karena masih banyak organisasi atau individu yang belum menerapkan kebijakan username dan password yang aman. Sehingga jenis serangan seperti *brute force attack* dan *social engineering* sangat mudah menjebol mekanisme otentikasi tunggal ini. Contohnya adalah dengan menggunakan kombinasi username dan password yang mudah di tebak dan tidak mengikuti kaidah-kaidah strong password. Kaidah strong password merupakan suatu petunjuk/ tips yang perlu di ikuti oleh user individu atau dalam sebuah organisasi dalam membuat username dan password yang sulit untuk di jebol.

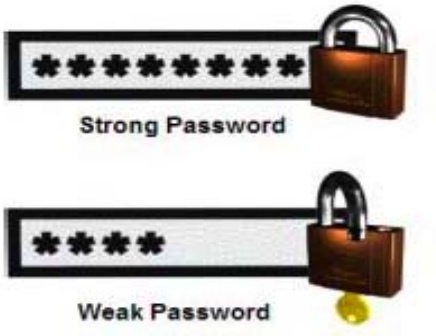
Berikut adalah petunjuk *strong password authentication*:

- Username default yang di buat oleh sistem secara otomatis sebaiknya di ganti untuk mencegah ditebak dengan mudah.
- Password yang berisikan kata-kata yang terdapat dalam kamus sebaiknya di hindari karena dapat di pecahkan dengan menggunakan program peenjebol password (password cracking).
- Password idealnya merupakan kombinasi dari huruf besar dan huruf kecil, angka, dan karakter khusus. Contoh karakter khusus adalah: %, !, dan &.



Gambar 2 Kombinasi karakter, angka, dan karakter khusus dalam password

- Password idealnya mudah di ingat tapi sulit untuk di tebak. Hindari penggunaan password lemah yang menggunakan pengenal pribadi seperti tanggal lahir, nama kecil. Contoh penggunaan strong password 12Ud!, yang mudah di ingat dengan menggunakan metode mnemonic rudi.



Gambar 3 strong passsword dan weak password

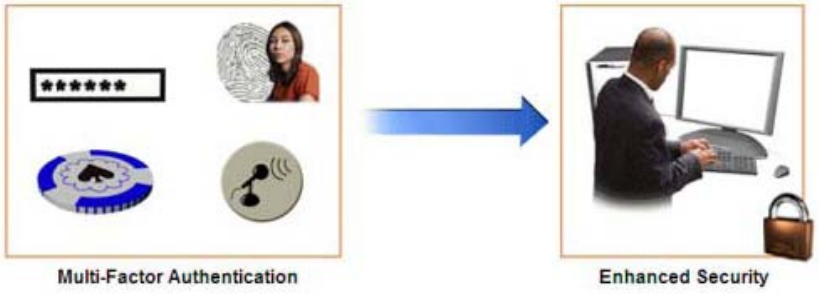
- Password yang kompleks sangat sulit untuk di ingat dan seringkali harus di tuliskan. Berilah pemahaman pada user jika menuliskan password maka harus di simpan pada tempat yang aman.
- Jika user memiliki password lebih dari satu untuk sistem jaringan dan situs web, biasanya mereka menyimpan daftar password tersebut dalam dalam sebuah file dalam sistem komputer mereka. Untuk melindungi file tersebut dari akses user yang tidak berhak, user seharusnya meng-enkripsi file tersebut dalam daftar passwordnya.
- Password harusnya terdiri dari minimal 8 karakter. Semakin banyak karakter yang di gunakan maka semakin sulit untuk menebak permutasi yang benar.
- Password yang digunakan untuk multiple sistem seperti sistem jaringan dan sistem web sebaiknya di buat unik satu sama lain.
- Password seharusnya di rubah secara berkala. Ini untuk mencegah penggunaan password secara permanen sehingga hal tersebut menyulitkan seorang *hacker* menebak perubahan berkala password tersebut.

Dari semua petunjuk diatas tentunya tidak dapat menjadi jaminan bahwa sistem komputer aman dari serangan pengacau. Untuk mengatasi masalah ini, maka di perlukan suatu mekanisme otentikasi yang lebih aman dan berlapis sehingga menyulitkan pengacau untuk mencoba mengakses sistem yang ada dalam sebuah organisasi secara tidak sah (ilegal). Mekanisme ini melibatkan banyak faktor-faktor pendukung dalam proses otentikasi yang biasa di sebut dengan “Multi Factor Authentication”.

Multi Factor Authentication

Gambar 4 Komponen dalam multi factor authentication

Otentikasi user dalam lingkungan jaringan di lakukan menggunakan faktor-faktor seperti password, token, dan biometrik. Ketika dua atau lebih faktor-faktor ini di gunakan untuk meng-otentikasi seorang user, otentikasi ini di sebut sebagai *multi factor authentication*.

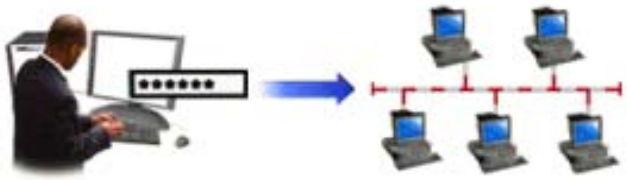


Gambar 5 Multi factor authentication menigkatkan keamanan

Multi factor authentication mampu meningkatkan keamanan karena menggunakan faktor-faktor lain sebagai tambahan untuk meng-otentikasi user. Faktor-faktor yang di gunakan dalam multi factor authentication di antaranya adalah: something you know, something you have, something you are, something you do.

Something You Know

Faktor something you know melibatkan pengetahuan informasi rahasia yang memungkinkan user meng-otentikasi dirinya sendiri ke sebuah server. Contoh dari faktor ini adalah sebuah password dan sebuah personal identification number (PIN).



Gambar 6 username dan password (something you know)

Something You Have

Faktor something you have melibatkan bahwa user harus memiliki alat secara fisik. Jika tanpa adanya alat tersebut maka user tidak dapat meng-otentifikasi dirinya sendiri ke server sistem computer. Contoh dari faktor ini menggunakan sebuah token dan smart card (kartu cerdas).

Gambar 7 token dan smart card (something you have)

Something You Are

Faktor something you are melibatkan bahwa user meiliki karakteristik yang unik yang membedakan dirinya dengan user lain untuk mengidentifikasi dirinya sendiri. Faktor ini menggunakan metode identifikasi biometrik untuk meng-otentikasi user. Contoh dari faktor something you are meliputi sidik jari, pemindaian retina mata, dan garis tangan seseorang.

Gambar 8 thumb print, retina scan, hand geometry (something you are)

Something You Do

Faktor something you do melibatkan bahwa tiap user ketika melakukan sesuatu atau ketika menggunakan sesuatu dengan cara yang berbeda. Contoh dari faktor ini penggunaan analisis suara (voice recognattion) atau analisis tulisan tangan.

Gambar 9 voice and hand writing analysis

Otentikasi multi faktor menyediakan lapisan keamanan tambahan dalam proses otentikasi. Lapisan tambahan ini mengurangi peluang yang bisa di lakukan oleh user yang tidak sah mencoba menerobos ke dalam sistem komputer. Selain keuntungan dari penggunaan otentikasi multi faktor, juga terdapat kelemahan dari mekanisme otentikasi ini.

Kelemahan Multi Faktor Otentikasi:

- Mungkin saja terjadi sebuiah situasi dimana seorang user yang berhak ternyata tidak dapat meng-otentikasi dirinya sendiri ke server sistem komputer menggunakan mekanisme ini. Misalnya, jika seorang user yang berhak kehilangan smart card mereka, maka user tersebut tidak dapat meng-otentifikasi dirinya sendiri ke dalam sistem komputer sampai smart card-nya tersebut di ganti/ di keluarkan lagi.
- Jika proses otentikasi user membutuhkan waktu yang cukup lama, user mungkin saja melewati beberapa tahap yang perlu untuk di lakukan atau bahkan user tidak mau lagi menggunakan proses otentikasi ini. Contohnya, jika sebuah pintu yang menggunakan kartu gesek memerlukan waktu yang cukup lama untuk mem-validasi kartu yang di miliki user tersebut, mungkin saja user tersebut akan tetap membiarkan pintu tersebut tetap terbuka. Ini mungkin saja membuka celah keamanan dari area aman gedung oleh user yang tidak berhak sehingga dapat menerobos ke dalam sistem komputer.
- Multi faktor otentikasi juga dapat menyebabkan membengkaknya biaya perawatan dari sistem komputer. Hal ini terjadi karena lebih banyak perangkat keras yang di butuhkan untuk mengimplementasikan proses otentikasi.

Kesimpulan

Penggunaan mekanisme otentikasi multi faktor mampu meningkatkan keamanan sistem komputer dalam proses otentikasi ke server di banding menggunakan otentikasi satu faktor saja (username dan password). Dengan multi faktor otentikasi sebuah organisasi dapat menjamin bahwa hanya user yang berhak dan terdaftar saja yang dapat masuk ke dalam sistem. Panduan penggunaan username dan password yang tepat sangat menentukan seberapa aman mekanisme ini di implementasikan. Satu hal yang perlu di pertimbangkan pada saat penerapan multi faktor otentikasi di sebuah organisasi adalah bahwa sistem ini masih memiliki beberapa kelemahan yang dapat mengakibatkan seorang user yang seharusnya berhak dapat saja di tolak untuk mengakses sistem komputer dalam organisasi tersebut.

Daftar Pustaka

- CompTIA Security+, Part 1 – security concepts., www.comptia.net
- Network Security Essentials., Stalling W., Prentice Hall., 2004
- Multi-Factor Authentication Solutions., www.soltrus.com., 2006.