PENGAMANAN WEBSITE E-COMMERCE MENGGUNAKAN MULTI-FACTOR AUTHENTICATION

Muhammad Adi Nugraha, Desi Arisandi [2], Novario Jaya Perdana [3]

[1) 2) 3)] Teknik Informatika Universitas Tarumanagara
Jl. Letjen S. Parman No. 1, Jakarta 11440 Indonesia
[1)]muhammad.535150088@stu.untar.ac.id [2)] desia@fti.untar.ac.id [3)] novariop@fti.untar.ac.id

ABSTRACT

Data security is very important and privacy for every user because there is sensitive information so it must be safe from irresponsible parties. One method that can secure user account data is Multi-Factor Authentication. E-commerce applications using Multi-Factor Authentication can secure their user accounts. This discussion is about creating website-based e-commerce applications that users can use to buy smart phone products. This E-commerce website application can secure users through 3 login steps. The login mechanism presented in this e-commerce website application is login with password, login with OTP code, and finally login with personal questions. The experimental results show that using the multi-factor authentication method provides good security for user accounts

Key words

E-commerce, Multi-Factor Authentication, Website

1. Pendahuluan

1.1 Latar belakang

Seiring dengan perkembangan teknologi informasi dan komunikasi, semua pekerjaan yang dilakukan oleh manusia perlahan-lahan terkomputerisasi. Hampir semua perusahaan besar dan menengah menerapkan teknologi informasi untuk membantu operasi bisnis mereka. Ada beragam hal yang sifatnya baru dalam dunia teknologi baik itu dinamis maupun inovatif merupakan ciri utamanya. Berdasarkan kebutuhan sehari-hari banyak yang tidak lepas dari teknologi.

Mengakses layanan berbasis web seperti e-commerce saat ini mengetikan nama pengguna dan kata sandi dimana kegiatan ini merupakan kerentanan karena kata sandi dapat diambil oleh pihak-pihak tertentu dan kemudian digunakan kembali oleh pihak yang tidak bertanggung jawab. Maka dibutuhkan lebih dari satu autentikasi yang dapat membantu dalam mengamankan akun pengguna.

Untuk mengatasi permasalahan diatas, maka perlu adanya rancangan sistem keamanan yang baik, salah satunya dengan memberikan layanan pengamanan menggunakan lebih dari satu proses autentikasi. Sehingga informasi pengguna lebih aman disimpan dan diproses oleh website

Salah satu sistem pengamanan yang akan membantu pada aplikasi yang dirancang yaitu autentikasi dimana sistem akan memeriksa pengguna untuk validasi akun pengguna.

Authentication adalah proses elektronik yang memungkinkan identifikasi elektronik dari seseorang atau badan hukum. Selain itu, autentikasi juga dapat mengkonfirmasi keaslian dan integritas data dalam bentuk elektronik, seperti penerbitan sertifikat digital untuk membuktikan keaslian sebuah situs web. Tujuan keseluruhan dari autentikasi adalah untuk mengurangi potensi penipuan, terutama jika seseorang dengan sengaja salah merepresentasikan identitasnya atau melalui penggunaan yang tidak sah atas kredensial orang lain. Dalam Authentication ada beberapa macam, salah satunya Multi-Factor Authentication. Dengan Multi-Factor Authentication memverifikasi identitas pengguna dengan menggunakan lebih dari dua faktor. Faktor-faktor yang digunakan biasanya adalah sesuatu yang diketahui pengguna seperti password atau passphrase atau PIN, dan sesuatu yang dimiliki pengguna seperti token atau sertifikat software, serta sesuatu yang berada di pengguna seperti personal security question atau sidik jari atau retina.

Dari setiap faktor dari Multi-Factor Authentication masing-masing memiliki keunggulan, diantaranya password yang mudah digunakan dan terhindar dari kerentanan karena terenskripsi melalui jaringan dan tidak pernah di simpan di klien, lalu token yang mudah dibuat dan lebih aman terhadap ancaman pengamanan karena muncul berdasarkan waktu dengan rumusan tertentu dan disinkronisasikan dengan server, serta personal security question yang sulit dipalsukan.

1.2 Tujuan dan Kegunaan

Tujuan perancangan pengamanan website e-commerce menggunakan multi-factor authentication adalah membuat sistem penjualan berupa e-commerce dan mengaplikasikan metode multifactor authentication untuk mengamankan penggunaan ecommerce dari serangan siber.

1.3 Batasan Rancangan

Implementasi Multi-Factor Authentication pada website e-commerce memiliki batasan rancangan sebagai berikut:

1. Aplikasi ini berupa e-commerce dengan sistem pengamanan multi-factor authentication.
2. Pemilihan mekanisme autentikasi seperti password, OTP (One Time Password) dan personal security question
3. Sistem pengamanan ini dilakukan hanya pada modul login.
4. Aplikasi ini memiliki 2 jenis hak akses, diantaranya hak akses admin pengelola sistem dan akses user.

2. Multi-Factor Authentication

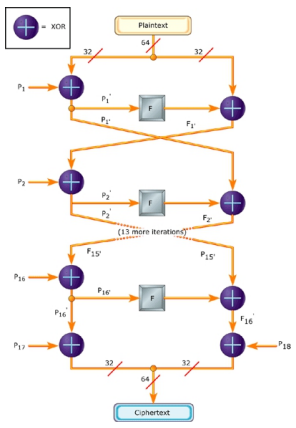
2.1 Password

Blowfish adalah symmetric-key block cipher, yang dirancang oleh Bruce Schneier, yang dikenal dengan key-independent S-Boxes yang besar dan key schedule yang sangat kompleks. Blowfish memiliki jaringan Feistel 16 putaran. Data round-spesific yang berasal dari chipper key disebut round key. Key schedule adalah algoritma yang menghitung semua round keys dari key. Blowfish memiliki ukuran blok 64-bit dan 32-bit hingga panjang kunci 448 bit

Untuk setiap round, algoritma Blowfish melakukan proses berikut:

1. XOR bagian kiri data dengan entri P-array ke-r.
2. Gunakan data XOR sebagai input untuk fungsi F Blowfish.
3. XOR keluaran fungsi-F dengan bagian kanan data.
4. Tukar L dan R.

Fungsi F Blowfish akan membagi masukan 32-bit menjadi empat perempat delapan bit. S-box akan mengubah kuarter yang panjangnya 8-bit menjadi 32-bit output. Kemudian, output ditambahkan modul 232 dan XOR untuk menghasilkan akhir 32-bit output.



Gambar 1 Algoritma Blowfish
Sumber : NehaKhatri Valmik, and V. K Kshirsagar, "Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2,(Mar-Apr. 2014), h.80

Berikut adalah langkah-langkah algoritma key schedule dalam Blowfish:

1. Inisialisasi P-array dan S-box dengan nilai yang diturunkan dari digit heksadesimal pi (12 digit pertama pi dalam heksadesimal 3.243F6A8885A3.....).
2. Byte demi byte, secret key di-XOR dengan semua entri-P secara berurutan.
3. 64-bit all-zero block kemudian dienkripsi dengan algoritma sebagaimana aslinya.
4. Ciphertext yang dihasilkan kemudian menggantikan P1 dan P2.
5. Ciphertext yang sama dienkripsi lagi dengan subkunci baru, dan ciphertext baru menggantikan P3 dan P4.
6. Proses ini akan terus menggantikan seluruh P-array dan semua S-box.

Algoritma blowfish akan berjalan 521 kali untuk menghasilkan semua subkunci. Blowfish hanya membutuhkan ruang RAM sekitar 4 KB. Penggunaan RAM yang kecil memungkinkan Blowfish untuk digunakan di sistem tertanam.

2.2 OTP

OTP adalah kode numerik yang dibuat secara acak dan unik selama setiap aktivitas autentikasi. Ini menambah lapisan keamanan tambahan, karena kata sandi yang dihasilkan adalah kumpulan digit baru setiap kali otentikasi dicoba dan menawarkan kualitas yang tidak dapat diprediksi untuk sesi yang dibuat berikutnya.

Contoh dari pembuatan OTP ini adalah Time Based OTP Algorithm (TOTP) yang dijelaskan sebagai berikut:

1. Server backend menghasilkan secret key.
2. Server berbagi secret key dengan layanan yang menghasilkan OTP
3. Kode otentikasi pesan berbasis hash (HMAC) dibuat menggunakan kunci rahasia dan waktu yang diperoleh. Ini dilakukan dengan menggunakan algoritma kriptografi SHA-1. Karena server dan perangkat yang meminta OTP, memiliki akses ke waktu, yang jelas dinamis, ini diambil sebagai parameter dalam algoritma. Di sini, stempel waktu Unix dianggap tidak bergantung pada zona waktu, yaitu waktu dihitung dalam detik mulai dari 1 Januari 1970. Mari kita pertimbangkan "0215a7d8c15b492e21116482b6d34fc4e1a9f6ba" sebagai string yang dihasilkan dari algoritma HMAC SHA1.
4. Kode yang dihasilkan panjangnya 20 byte dan dengan demikian dipotong sesuai panjang yang

diinginkan untuk dimasuki pengguna. Disini pemotongan dinamis digunakan. Untuk kode 20-byte "0215a7d8c15b492e21116482b6d34fc4e1a9f6ba", setiap karakter menempati 4 bit. Seluruh string diambil sebagai 20 string satu byte individu.

5. Penghitung digunakan untuk melacak waktu yang telah berlalu dan menghasilkan kode baru setelah interval waktu yang ditentukan
6. OTP yang dihasilkan dikirim ke pengguna dengan metode yang dijelaskan di atas.
7. OTP yang digunakan menggunakan library PHP Ghangsta

2.3 Personal Security Question

Personal Security Question adalah salah satu metode untuk memverifikasi pengguna dengan menjawab pertanyaan tertentu yang jawabannya hanya diketahui oleh pengguna secara personal. Ketika pengguna membuat akun, pengguna memberikan jawaban atas pertanyaan yang bersifat pribadi. Idealnya, sebuah pertanyaan yang hanya pengguna yang tahu jawabannya. Jawaban itu dicatat, dan jika pengguna perlu mengonfirmasi bahwa pengguna adalah pemegang akun yang sah, sistem menanyakan pertanyaan itu kepada pengguna. Jika jawaban pengguna cocok dengan yang saat pengguna masukkan pada saat membuat akun, pengguna masuk sebagai pemegang akses. Meski terlihat sederhana, memilih dan mengisi jawaban personal security questions sama pentingnya dengan ketika membuat kata sandi.

Banyak masalah dapat diselesaikan dengan menggunakan pertanyaan keamanan yang baik yang memenuhi lima kriteria. Pertanyaan keamanan yang baik adalah:

1. Aman : tidak bisa ditebak atau diteliti. Karakteristik terpenting dari pertanyaan keamanan yang baik adalah keamanan. Pertanyaan ini tidak membahayakan hal yang coba dilindungi.
2. Stabil : tidak berubah seiring waktu. Jawaban atas pertanyaan keamanan yang baik tidak berubah seiring waktu.
3. Memorable : Pertanyaan keamanan harus mudah diingat tetapi masih belum diketahui untuk orang lain. Idealnya, pengguna harus segera mengetahui jawabannya tanpa mencari referensi atau harus menuliskan jawabannya. Contoh buruk yaitu “Berapa nomor SIM Anda?” (belum menghafal). Pertanyaan masa kecil bisa jadi sulit bagi orang tua. Gunakan pertanyaan yang lebih menonjol atau mudah diingat.
4. Sederhana : Pertanyaan harus ditanyakan sehingga jawabannya pasti, sederhana dan tepat, akan dijawab secara konsisten dengan cara yang sama, dan tidak peka huruf besar kecil.
5. Banyak : Pertanyaan yang bagus akan memiliki banyak kemungkinan jawaban, semakin banyak jawaban yang mungkin, semakin baik keamanannya. Ini bukan hanya masalah seseorang menebak, tetapi juga mencoba menghentikan upaya otomatis. Ratusan ribu atau lebih opsi lebih baik daripada beberapa ratus.

3. Hasil Pengujian

Pada tahap ini akan dilakukan pengujian terhadap enkripsi kata sandi dan OTP. Pengujian enkripsi kata sandi di uji dengan memecahkan kata sandi yang sudah di enkripsi dengan cara dictionary attack melalui tools password cracked yaitu hashcat. Dictionary attack dilakukan dengan menyediakan sekumpulan password yang paling memungkinkan digunakan, dengan daftar password yang telah disiapkan, selanjutnya mengeliminasi setiap daftar yang telah dicoba dan gagal. Pada pengujian OTP diuji dengan beberapa test case yang dilakukan bersama dosen pembimbing

3.1 Pengujian Password

Berdasarkan pengujian terhadap enkripsi kata sandi dengan password cracker, dengan 3 password yang terenkripsi dijalankan proses dictionary attack dengan wordlist lebih dari 13 juta karakter selama lebih dari 12 jam serta lebih dari 1 juta percobaan menghasilkan enkripsi kata sandi dengan blowfish tidak terpecahkan.

Gambar 2 Cracking blowfish

Hasil pengujian test case login menghasilkan hasil yang berhasil berfungsi dengan baik.

Tabel 1 Test case login

No	Pengujian	Sukses	Gagal
1	Berhasil login dengan menggunakan nama pengguna dan kata sandi yang benar	V	
2	Gagal melakukan login dengan akun yang belum terdaftar	V	
3	Gagal melakukan login dengan	V	

	nama pengguna yang benar dan kata sandi yang salah		
4	Gagal melakukan login dengan nama pengguna yg salah dan kata sandi yang benar	V	
5	Gagal melakukan login dengan nama pengguna dan kata sandi dikosongkan	V	
6	Gagal masuk sebagai pengguna website saat nama pengguna atau kata sandi menggunakan huruf besar saat data sebenarnya huruf kecil	V	

3.2 Pengujian OTP

Hasil pengujian test case OTP dengan beberapa kategori diantaranya kode OTP terkirim ke email akun pengguna yang sudah terdaftar, kode OTP akan kadaluarsa pada waktu tertentu, kode OTP hanya dikirimkan ke email pengguna, kode OTP yang kadaluarsa tidak dapat digunakan, pengiriman ulang kode OTP berfungsi dengan baik, kode OTP lama tidak akan valid jika pengguna meminta ulang kode OTP yang baru, kode OTP yang diberikan terbatas yaitu 3 kali pengiriman, akun pengguna akan di ban untuk beberapa waktu, saat sudah melebihi batas mengirim ulang kata sandi yang dilakukan menghasilkan hasil yang berhasil berfungsi dengan baik.

Tabel 2 Test case OTP

No	Pengujian	Sukses	Gagal
1	Kode OTP terkirim ke email pengguna	V	
2	Kode OTP akan kadaluarsa pada waktu tertentu	V	
3	Kode OTP hanya dikirimkan ke email pengguna	V	
4	Kode OTP yang kadaluarsa tidak dapat digunakan	V	
5	Pengiriman ulang kode OTP berfungsi dengan baik	V	
6	Kode OTP lama tidak akan valid jika pengguna meminta ulang kode OTP yang baru	V	
7	Kode OTP yang diberikan terbatas yaitu 3 kali pengiriman	V	
8	Akun pengguna akan di *ban* untuk beberapa waktu, saat sudah melebihi batas mengirim ulang kata sandi	V	

4. Kesimpulan

Kesimpulan yang dapat diperoleh berdasarkan pembuatan dan pengujian dari aplikasi pengamanan website e-commerce menggunakan Multi-Factor Authentication yaitu:

1. Aplikasi Login Multi-Factor Authentication ini sudah berfungsi dengan baik sesuai dengan spesifikasi rancangan.
2. Hasil dari enkripsi kata sandi dengan algoritma blowfish dapat mengamankan kata sandi dengan baik.
3. Hasil dari pengujian OTP dapat disimpulkan bahwa akun pengguna akan aman dan sudah berfungsi dengan baik.
4. Berdasarkan hasil pengujian diketahui bahwa Pengamanan Website E-commerce menggunakan Multi-Factor Authentication memberikan akun pengguna aman.

REFERENSI

[1] Stallings, Willam. “Cryptography and network security : Principles and Practice”. (New York: Prentice Hall, 2006), h. 37.

[2] Richard Kissel et al., “Security Considerations in the System Development Life Cycle”, NIST Special Publication 800-64 Revision 2(October 2008), h.11.

[3] Neha Khatri Valmik, and V. K Kshirsagar, "Blowfish Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2,(Mar-Apr. 2014), h.80.

[4] Garska, Kathleen. Two-Factor Authentication (2FA) Explained: One Time Password Soft Tokens. https://blog.identityautomation.com/two-factor-authentication-2fa-explained-one-time-password-soft-tokens, 25 September 2020.

[5] InfoGuardSecurity. WHAT IS INFORMATION SECURITY? DEFINITION, PRINCIPLES, AND POLICIES. https://www.infoguardsecurity.com/what -is-information-security-definition-principles-and-policies/, 17 September 2020.

[6] Loginradius. Multi-Factor Authentication (MFA): What is it and Why Do You Need it?.https://www.loginradius.com/blog/2019/06/what-is-multi-factor-authentication/, 14 September 2020.

[7] Idcloudhost. Pengertian E-Commerce dan Contohnya, Komponen, Jenis, dan Manfaat E-Commerce. https://idcloudhost.com/pengertian-e-commerce-dan-contohnya-komponen-jenis-dan-manfaat-e-commerce/, 3 September 2020

Muhammad Adi Nugraha, saat ini adalah mahasiswa tingkat akhir Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Tarumanagara, Jakarta.

Desi Arisandi, memperoleh gelar S.Kom dari Universitas Tarumanagara. Kemudian memperoleh gelar M.TI dari Universitas Indonesia. Saat ini sebagai Staf Pengajar program studi Teknik Informatika Universitas Tarumanagara.

Novario Jaya Perdana, memperoleh gelar S.Kom dari Institute Teknologi Sepuluh November. Kemudian memperoleh gelar M.T dari Universitas Indonesia. Saat ini sebagai Staf Pengajar program studi Teknik Informatika Universitas Tarumanagara