PENERAPAN HMAC BASED ONE TIME PASSWORD (HOTP) UNTUK MENDUKUNG MEKANISME LOGIN

Skripsi

oleh
HELFY DINAULIK
22094758

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2018

PENERAPAN HMAC BASED ONE TIME PASSWORD (HOTP) UNTUK MENDUKUNG MEKANISME LOGIN

Skripsi

Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

HELFY DINAULIK
22094758

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2018

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PENERAPAN HMAC BASED ONE TIME PASSWORD (HOTP) UNTUK MENDUKUNG MEKANISME LOGIN

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 4 Januari 2018

HELFY DINAULIK
22094758

HALAMAN PERSETUJUAN

Judul Skripsi	: PENERAPAN HMAC BASED ONE TIME PASSWORD (HOTP) UNTUK MENDUKUNG MEKANISME LOGIN
Nama Mahasiswa	: HELFY DINAULIK
N I M	: 22094758
Mulakuliah	: Skripsi (Tugas Akhir)
Kode	: TIW276
Semester	: Gasal
Tahun Akademik	: 2017/2018

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 21 November 2017

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Budi Susanto, SKom.,M.T.

HALAMAN PENGESAHAN

PENERAPAN HMAC BASED ONE TIME PASSWORD (HOTP) UNTUK MENDUKUNG MEKANISME LOGIN

Oleh: HELFY DINAULIK / 22094758

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 18 Desember 2017

Yogyakarta, 4 Januari 2018
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom., M.Cs.
2. Budi Susanto, SKom., M.T.
3. Antonius Rachmat C., S.Kom., M.Cs.
4. Laurentius Kuncoro Probo Saputra, S.T., M.Eng.

Dekan

(Budi Susanto, S.Kom., M.T.)

Ketua Program Studi

(Gloria Virginia, Ph.D.)

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih terutama Tuhan Yesus Kristus yang membuka jalan agar penelitian ini bisa berjalan dengan baik dan Dosen pembimbing I Willy Sudiarto Raharjo yang telah memberi saran penelitian sehingga penulis dapat kemudian melakukan penelitian ini serta kepada Dosen Pembimbing II Budi Susanto yang telah memberikan saran ruang lingkup untuk batasan penelitian dari saran Dosen pembimbing I , teman-teman seperjuangan yang sudah memberi dukungan dan bantuan pengetahuan serta tetap saling mengingatkan untuk tetap semangat tentunya dalam mengerjakan penelitian.

INTISARI

PENERAPAN HMAC-*BASED ONE TIME PASSWORD* (HOTP) UNTUK MENDUKUNG MEKANISME *LOGIN*

Penelitian tentang mekanisme login menggunakan prokotokol *H-mac Based One Time Password* (HOTP) ini sudah dapat diterapkan sesuai dengan yang penulis harapkan dengan beberapa masalah seperti penetapan durasi waktu yang digunakan dalam masa valid, waktu yang diperlukan dalam mengirim kode OTP (One Time Password) ke *handphone user* dan kode OTP yang dipakai diluar masa valid berhasil dijalankan.

Dalam penelitian lain yang juga menerapkan *password* sekali pakai yaitu menggunakan protokol Time Based One time password (TOTP) juga sudah berhasil diterapkan, sumber kode yang digunakan dihasilkan oleh google autentikator. Perbedaan dari metode *H-mac Based One Time Password* (HOTP) dan *Time Based One Time Password* (TOTP) adalah terletak pada masa valid nilai kode, sesuai dengan namanya protokol TOTP memiliki waktu yang lebih singkat yakni 30 detik karena berdasarkan waktu, sedangkan HOTP dalam penentuan waktunya lebih fleksibel namun harus ditetapkan berdasarkan ujicoba pengiriman kode OTP dalam studi kasus ini menggunakan SMS gateway.

HOTP ini digunakan sebagai metode untuk mengkalkulasi nilai kode OTP (One Time Password) dan menjadi salah satu cara untuk meningkatkan keamanan pada sistem login.

Kata kunci : HOTP ,SHA-1, SMS Gateway

DAFTAR ISI

INTISARI

PENERAPAN HMAC-*BASED ONE TIME PASSWORD* (HOTP) UNTUK MENDUKUNG MEKANISME *LOGIN*

Penelitian tentang mekanisme login menggunakan prokotokol *H-mac Based One Time Password* (HOTP) ini sudah dapat diterapkan sesuai dengan yang penulis harapkan dengan beberapa masalah seperti penetapan durasi waktu yang digunakan dalam masa valid, waktu yang diperlukan dalam mengirim kode OTP (One Time Password) ke *handphone user* dan kode OTP yang dipakai diluar masa valid berhasil dijalankan.

Dalam penelitian lain yang juga menerapkan *password* sekali pakai yaitu menggunakan protokol Time Based One time password (TOTP) juga sudah berhasil diterapkan, sumber kode yang digunakan dihasilkan oleh google autentikator. Perbedaan dari metode *H-mac Based One Time Password* (HOTP) dan *Time Based One Time Password* (TOTP) adalah terletak pada masa valid nilai kode, sesuai dengan namanya protokol TOTP memiliki waktu yang lebih singkat yakni 30 detik karena berdasarkan waktu, sedangkan HOTP dalam penentuan waktunya lebih fleksibel namun harus ditetapkan berdasarkan ujicoba pengiriman kode OTP dalam studi kasus ini menggunakan SMS gateway.

HOTP ini digunakan sebagai metode untuk mengkalkulasi nilai kode OTP (One Time Password) dan menjadi salah satu cara untuk meningkatkan keamanan pada sistem login.

Kata kunci : HOTP ,SHA-1, SMS Gateway

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Internet pada masa sekarang sudah sebagai sarana utama diberbagai aktivitas. Salah satu contoh adalah penyimpanan data pada media yang terhubung pada jaringan internet. Ini akan menjadi sesuatu yang bisa mempermudah semua pihak yang terkait dalam hal mengakses, mengolah, dan mengambil data tersebut. hal yang penting untuk diperhatikan yaitu dengan adanya sistem jaringan menggunakan komputer dan menjadi masalah adalah keamanannya. Banyak komputer yang bisa terhubung dengan jaringan dan banyak juga *user* yang menggunakan untuk berbagai kepentingan. suatu data maupun informasi menjadi sangat rentan terhadap serangan-serangan dari pihak-pihak yang tidak berhak.

Untuk itu perlu adanya keamanan yang bisa mencegah hal tersebut terjadi. Salah satu cara yaitu dengan pemberian *password*. Metode autentikasi dengan menggunakan *password* biasa dapat dikatakan statis dan sangat umum. *Password* akan bisa riskan jika tidak diganti secara berkala. Salah satu bentuk serangan ke sistem komputer jaringan adalah seseorang mencoba masuk ke dalam suatu koneksi jaringan untuk mendapatkan informasi autentikasi, seperti ID *login* dan *password* yang berbeda setiap kali user akan masuk ke sistem.

Untuk itu penulis mencoba untuk mengatasi masalah tersebut dengan menggunakan *One Time Password* yaitu dimaksudkan agar *password* yang dipakai oleh *user* bisa selalu berbeda. Dengan menggunakan metode *HMAC Based one time Password* (HOTP). HOTP sendiri akan memberikan nilai *one time password* yang dihasilkan berupa n-digit *integer* yang dapat diatur panjang digit *password I (*misal 6 digit) pada *input* dari fungsi itu. One time *password*

dapat menghitung nilai dari input berupa sebuah *counter* yang akan divalidasi dari *server* dengan *client*. Untuk proses autentikasi dengan HOTP, mesin dari HOTP ini akan dimasukkan ke dalam *server*. setiap saat user melakukan *request* untuk menjalankan HOTP, maka nilai HOTP akan dikirim ke perangkat *client* melalui SMS *gateway* (melalui SMS ke nomor *handphone*).

1.2. Rumusan Masalah

Untuk mendukung mekanisme login menggunakan OTP bisa ditemukan rumusan sebagai berikut :

1. Waktu yang diperlukan agar kode OTP bisa sampai ke user menggunakan sms gateway.
2. Penentuan durasi masa valid kode OTP untuk bisa diverifikasi oleh server.
3. Penggunaan kode OTP diluar masa valid.

1.3. Batasan Masalah

Adapun batasan masalah digunakan untuk mencegah meluasnya topik, untuk itu beberapa batasan masalah pada topik ini sebagai berikut :

1. Algoritma yang digunakan untuk mendapatkan kode OTP adalah HOTP .
2. Penulis akan menggunakan *library One-time password library for HMAC-based (HOTP).*
3. Penelitian ini difokuskan pada proses login.
4. Pengiriman kode OTP dari *server* ke *user* melalui SMS dengan SMS gateway – gammu.

1.4. Tujuan

Tujuan yang ingin dicapai adalah sebagai berikut :

1. Memastikan bahwa proses verikasi kode OTP dengan protokol *H-mac Based One Time Password* HOTP bisa digunakan untuk meningkatkan keamanan dari sebuah proses login.

1.5. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah:

1. Studi Pustaka

   Membaca dan mempelajari artikel-artikel yang terkait dengan topik ini

2. Wawancara

   Metode ini dilakukan dengan melakukan tanya jawab dengan beberapa responden yang berpengalaman dalam bidang ini.

3. Analisis kebutuhan perangkat lunak

   Metode ini dilakukan dengan cara menganalisis data apa saja yang diperlukan untuk mendukung mekanisme yang akan berjalan.

4. Perancangan perangkat lunak

   Perancangan untuk sistem ini dengan membangun sistem database dalam studi kasus data presensi mahasiswa yang diberikan proses login.

5. Implementasi

   Menerapkan hasil perancangan perangkat lunak untuk membangun aplikasi OTP dengan menggunakan protokol HOTP dengan pengiriman kode password melalui sms gateway.

1.6. Sistematikan Penulisan

Secara garis besar tugas akhir ini terdiri dari 5 bab dengan beberapa sub bab.untuk mempermudah arah dan gambaran yang jelas mengenai hal yang tertulis, berikut ini sistematika penulisannya:

Bab 1, Pendahuluan yang memberikan gambaran secara umum mengenai apa yang diteliti dalam tugas akhir ini. Pada bab ini membahas latar berlakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

Bab 2, Landasan teori, tinjauan pustaka berisi uraian berbagai teori mengenai one time password, SMS gateway dan metode HMAC *based one time*

password yang didapatkan dari berbagai sumber pustaka beserta contoh kasusnya yang digunakan untuk penyusunan tugas akhir.

Bab 3, Analisis dan perancangan sistem, yang mencakup perancangan sistem yang akan dibuat, yakni mengenai kebutuhan *hardware* dan *software*, bahan atau materi, *usecase diagram*, metode yang digunakan, pengumpulan data dan rancangan antarmuka sistem.

Bab 4, Implementasi dan analisis sistem yang memuat hasil riset implementasi dan pembahasan mengenai sistem yang sifatnya terpadu berdasarkan bab 3, beserta hasil dari sistem yang dijalankan dan analisis dari sistem yang dibuat.

Bab 5, Kesimpulan dan saran, yang berisi kesimpulan dari hasil penelitian yang didapatkan dan saran untul memberikan analisis dan pengembangan yang akan lebih baik lagi dari pada penelitian kedepannya dalam topik yang serupa.

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Sistem login kedua menggunakan HOTP (HMAC based *One Time Password*) sudah berhasil diterapkan. Dalam penerapannya dapat menghasilkan kode OTP atau sebagai password sekali pakai untuk mendukung keamanan dari sistem yang memerlukan mekanisme login ini. Melalui beberapa pengujian yang sudah diujicobakan pada Bab 4 dapat disimpulkan, yaitu :

1. Waktu paling lama yang diperlukan berdasarkan pengujian ke provider yang berbeda adalah 41,93 detik.
2. Penentuan Durasi masa valid berdasarkan Pengujian pengiriman sms ke provider berbeda, sehingga penulis menentukan waktu 3 menit agar user masih memiliki waktu yang cukup untuk mengisi kode OTP ke form login.
3. Kode OTP tidak dapat digunakan lagi ketika sudah dipakai sekali untuk proses login.

5.2 Saran

Saran untuk pengembangan sistem ini sebagai perbaikan untuk penelitian lebih lanjut adalah sebagai berikut :

1. Waktu pengiriman kode OTP ke user masih bisa dikaji ulang dengan melakukan ujicoba pengiriman dengan berbagai waktu dan berbeda provider. Dimaksudkan supaya waktu yang ditentukan tidak terlalu cepat dan tidak terlalu lama, mengingat pengiriman kode melalui jaringan SMS gateway.

2. Perlu adanya peringatan ketika user melakukan beberapa kali login gagal.
3. Proses login menggunakan OTP ini hanya untuk mendukung mekanisme login saja, sehingga untuk kedepannya dapat diterapkan untuk sistem sebenarnya yang membutuhkan login.

Daftar Pustaka

Amirullah, (2006). "Aplikasi Sms Gateway Dengan Protokol Smpp (Short Message Peer-To-Peer) Pada Personal Computer ",Skripsi STMIK AKAKOM Yogyakarta.

Artikel teknik informatika dan Sistem Informasi (2017). SMS Gateway. Diakses pada tanggal 18 mei 2017, dari http://informatika.web.id/short-message-service.htm#more-1252.

D.Santhi, Jeslet., Sivaraman, G., Uma M., Thangadurai, K., Punithavalli, M., (2010). *Survey on Awareness and security Issues in Password Management Strategies, IJCSNS*

Elrod, R. (2005), *Two Factor Authentication*. Diakses pada 20 mei 2017, dari http://www.infosecwriters.com/text_resources/pdf/Two_Factor_Authentication.pdf

Fakhrusy, Muhamad., (2016). "Implementasi HMAC-SHA-3-Based One Time Password pada Skema Two-Factor Authentication", Jurnal, Bandung: Institut Teknologi Bandung.

Forque, P.-A., Leurent, G., Real, D., & Valette, F.(2009), *Pratical Electromagnetic Template Attack on HMAC*. Diakses November 2017, dari https://who.rocq.inria.fr/Gaetan.Leurent/files/HMAC_CH09.pdf

Halim, Meliana. (2014). " Desain dan Implementasi Aplikasi One-time Password Dengan Metode Advanced Encryption Standard Berbasis Perangkat Bergerak", Malang.

Huang, Chun-Ying., Ma, Shang-Pin., Chen, Kuan-Ta, (2011). Diakses November 2017 dari Using One Time Password to prevent password phising attacks. Journal of Networkand Computer Applications [JNCA] www. Elsevier.com/locate/jnca

Kovac, E. (2015). *New Collision Attack Lowers Cost of Breaking SHA1* Diakses pada tanggal 18 mei 2017, dari

http://www.securityweek.com/new-collision-attack-lowers-cost-breaking-sha1

Kristiyan, Wendroandy. (2009). "Penerapan One Time Password Menggunakan Sms Gateway Pada Aplikasi Forum Diskusi", Yogyakarta.

M. Pei J. Rydell D.M'Raihi, S. Machani., (2011) Totp: *Time-based one-time password algorithm.* Request for Comments: 6238.

-Patterson, K. G., & Stebila, D. (2009). *One time Password-Authentication Key Exchange*. November 2017 dari https://link.springer.com/chapter/10.1007/978-3-642-14081-5_17

Putri, Rhyca A, dkk. (2013). " Pemanfaatan SMS Gateway Dalam Pelayanan Informasi Aktifitas Siswa Pada Tk Xaverius 5 Palembang", Palembang.

Setiawan, Tjandrayana., (2016). Pengembangan Sistem Two Factor Authentication Menggunakan Protokol Time-Based One Time Password, Skripsi, Yogyakarta: Universitas Kristen Duta Wacana.

Wijaya, Tesar Ardan, Purwanti Desi., (2012). Sistem *Two-Factor Authentication* Dengan *Algoritma Time-Based One-Time Password* Pada Aplikasi Web Menggunakan Perangkat Android, Jurnal skripsi, Semarang: Universitas Dian Nuswantoro.