STUDI LITERATUR: PEMANFAAT ONE TIME PASSWORD (OTP) DAN ALGORITMA HMAC-SHA1 PADA USB DEVICE UNTUK PROSES AUTHENTICATION

Skripsi

oleh
OBETH PASANDA
22043632

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

STUDI LITERATUR: PEMANFAAT ONE TIME PASSWORD (OTP) DAN ALGORITMA HMAC-SHA1 PADA USB DEVICE UNTUK PROSES AUTHENTICATION

Skripsi

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

Disusun oleh

OBETH PASANDA
22043632

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

STUDI LITERATUR: PEMANFAAT ONE TIME PASSWORD (OTP) DAN ALGORITMA HMAC-SHA1 PADA USB DEVICE UNTUK PROSES AUTHENTICATION

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik 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, 1 Agustus 2013

OBETH PASANDA
22043632

HALAMAN PERSETUJUAN

Judul Skripsi	:	STUDI LITERATUR: PEMANFAAT ONE TIME PASSWORD (OTP) DAN ALGORITMA HMAC-SHA1 PADA USB DEVICE UNTUK PROSES AUTHENTICATION
Nama Mahasiswa	:	OBETH PASANDA
N I M	:	22043632
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2012/2013

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 1 Agustus 2013

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Nugroho Agus Haryono, M.Si

HALAMAN PENGESAHAN

STUDI LITERATUR: PEMANFAAT ONE TIME PASSWORD (OTP) DAN ALGORITMA HMAC-SHA1 PADA USB DEVICE UNTUK PROSES AUTHENTICATION

Oleh: OBETH PASANDA / 22043632

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 15 Agustus 2013

Yogyakarta, 21 Agustus 2013
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Nugroho Agus Haryono, M.Si
3. Budi Susanto, SKom.,M.T.
4. Junius Karel, M.T.

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada **Tuhan Yang Maha Esa** atas segala rahmat dan karunia serta pertolongan-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Studi Literatur: Pemanfaat *One Time Password (OTP)* dan Algoritma *HMAC-SHA1* pada *Usb Device* untuk Proses *Authentication*".

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu bertujuan melatih mahasiswa untuk dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan program dan penyusunan laporan Tugas Akhir ini penulis telah banyak mendapatkan masukan dan bimbingan dari berbagai pihak untuk kelacaran penyelesaian penulisan Tugas Akhir ini. Untuk itu pada kesempatan ini penulis menyampaikan ucapan terimakasih kepada :

1. **Tuhan Yesus Kristus** yang telah memberikan hikmat, jalan keluar, pertolongan-pertolongan pada waktu-NYA dan semangat serta kekuatan baru dalam mengerjakan Tugas Akhir ini hingga selesai.
2. Bapak **Willy Sudiarto Raharjo, SKom.,M.Cs** selaku dosen pembimbing I yang telah banyak meluangkan waktunya memberikan pengarahan dan saran dari awal sampai terselesaikannya Tugas Akhir ini.
3. Bapak **Nugroho Agus Haryono, M.Si** selaku dosen pembimbing II yang telah banyak memberi bimbingan dan petunjuk serta masukan–masukan dalam pembuatan Tugas Akhir ini.
4. Keluarga tercinta yang telah memberikan dukungan dan semangat.
5. Teman-teman yang telah memberikan masukkan, dukungan doa dan semangat.

Penulis menyadari bahwa laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca, supaya suatu saat penulis dapat menghasilkan suatu karya yang lebih baik dan bermanfaat bagi pengguna.

Akhir kata penulis mohon maaf yang sebesar-besarnya apabila ada kesalahan selama penyusunan Tugas Akhir ini. Semoga Tugas Akhir ini dapat bermanfaat bagi kita semua.

Yogyakarta, 02 Agustus 2013

Penulis

ABSTRAK

STUDI LITERATUR: PEMANFAAT *ONE TIME PASSWORD (OTP)* DAN ALGORITMA *HMAC-SHA1* PADA *USB DEVICE* UNTUK PROSES *AUTHENTICATION*

Untuk menjaga keamanan dan kerahasian data yang kita miliki pada sebuah *website* dibutuhkan perhatian khusus untuk penggantian *password* yang kita miliki secara berkala, sehingga mencegah kerugian yang akan terjadi karena data yang kita miliki diambil secara ilegal.

One Time Password (*OTP*) merupakan salah satu pemecahan masalah dimana kita tidak perlu mengganti *password* yang kita miliki pada sebuah *website* karena *OTP* merupakan *password* yang dapat digunakan hanya sekali, alat yang menghasilkan *OTP* disebut *token*. *Hash-based Message Authentication Code - Secure Hash Algorithm* 1 (*HMAC-SHA1*) merupakan algoritma yang digunakan untuk menghasilkan *OTP*. Penulis akan membahas konsep serta pemanfaat *OTP* dan algoritma *HMAC-SHA1* pada sebuah *token* dalam bentuk sebuah *usb device* yang digunakan untuk proses *authentication*.

Dari penelitian ini, penulis berharap pembaca dapat memahami: penerapan *OTP* dan algoritma *HMAC-SHA1*, alur untuk proses *authentication* serta permasalahan keamanan yang kemungkinan akan terjadi pada sistem yang menerapkan *OTP* yang menggunakan algoritma *HMAC-SHA1*.

Kata kunci : Kriptografi, *One Time Password (OTP)*, *Hash-based Message Authentication Code - Secure Hash Algorithm* 1 (*HMAC-SHA1*).

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet merupakan salah satu penemuan dalam teknologi komputer yang pada saat sekarang ini memiliki kemajuan dengan sangat cepat, penggunaan internet mulai dari penyebaran informasi, komersial, hiburan, organisasi hingga jejaringan sosial. Pengetahuan mengenai keamanan komputer merupakan hal yang sangat penting untuk menjaga keamanan sebuah sistem dan kerahasiaan data yang berada pada jaringan internet.

Keamanan komputer menjadi salah satu fokus dalam sebuah sistem di berbagai bidang dan berbagai alat yang digunakan dalam melakukan pertukaran data atau informasi seperti: *desktop, tablet pc* dan telepon genggam. Pengamanan data atau informasi dapat dilakukan dengan mencegah agar data atau informasi yang digunakan tidak dapat dibaca, dimodifikasi atau direkayasa sehingga tidak terjadi penyalahgunaan data yang ada. Kriptografi merupakan ilmu dalam bidang keamanan komputer yang dapat melakukan hal di atas.

Pada penulisan tugas akhir ini penulis akan menjelaskan mengenai pemanfaat beserta perhitungan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* yang dapat digunakan pada proses *authentication* beberapa sistem komputer pada integrasi sistem untuk meningkatkan keamanan dalam sebuah sistem seperti pada *Single Sign-On* untuk menggunakan beberapa layanan web, *Content Management System* (*CMS*) seperti *WordPress* dan *Blogger* (*Blogspot*), *Disk Encryption*, *Secure Secrets on Servers* untuk mengamankan *secrets* atau data yang penting dalam sebuah *server*, layanan internet (*e-mail, PayPal, LiveJournal* dan *Flickr*).

1.2 Perumusan Masalah

Dari latar belakang di atas, maka penulis dapat merumuskan permasalahan sebagai berikut:

a. Bagaimanakah pemanfaatan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* untuk proses *authentication*?
b. Apa saja permasalahan keamanan yang kemungkinan akan terjadi pada sistem yang menerapkan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* untuk proses *authentication*?

1.3 Batasan Masalah

Berdasarkan perumusan masalah di atas, maka penulis membatasi perumusan masalah berdasarkan sumberliteratur adalah sebagai berikut :

a. Penulis membahas *workflow* atau alur kerja dalam sistem yang menggunakan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* untuk proses *authentication*.
b. Penulis menggunakan contoh kasus pada **Yubico** sebuah perusahaan yang mengembangkan perangkat lunak dan perangkat keras yang memanfaatkan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1*.
c. Mode *One Time Password* (*OTP*) yang diteliti adalah *event synchronous*/ *event based*.
d. Algoritma yang digunakan adalah *HMAC-SHA1* yang diterapkan pada konsep *One Time Password* (*OTP*) yang menghasilkan *HOTP* (*HMAC-Base One-Time Password*).

1.4 Tujuan Penelitian

Tujuan dibuatnya penulisan ini adalah sebagai berikut :

a. Mengetahui *workflow* atau alur kerja sistem yang memanfaatkan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* untuk proses *authentication*.

b. Sebagai salah satu referensi untuk mahasiswa yang ingin membangun sistem (aplikasi atau perangkat lunak) yang menggunakan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* ke dalam sebuah *USB Device* untuk proses *authentication*.

1.5 Metode Penelitian

Metodologi yang digunakan dalam penelitian ini :

a. Metode Studi Literatur

   Studi literatur dilakukan dengan mengumpulkan sumber-sumber literatur dari jurnal, buku dan situs yang membahas mengenai *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1*.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini dibagi dalam beberapa bab yang setiap bab memiliki isi, yaitu:

BAB 1 PENDAHULUAN berisi tentang latar penjelasan belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB 2 TINJAUAN PUSTAKA berisi uraian dari konsep-konsep atau teori-teori yang dipakai sebagai dasar penulisan ini beserta sejarah kriptografi, *HMAC-SHA1* dan *One Time Password* (*OTP*) yang terdiri dari tinjauan pustaka dan landasan teori.

BAB 3 STUDI LITERATUR berisi tentang contoh penerapan *One Time Password* (*OTP*) pada sistem secara umum (distandarkan oleh **RSA Security**), langkah-langkah perhitungan algoritma *HMAC-SHA1* dan penerapan *HMAC-SHA1* pada *IPSec*.

BAB 4 PEMBAHASAN berisi tentang penerapan *One Time Password* (*OTP*) pada sistem **Yubico**, contoh perhitungan *SHA-1*, contoh perhitungan *HMAC-SHA1*, contoh perhitungan *HMAC-SHA1* yang diterapkan pada *One Time Password* (*OTP*) yang disebut dengan *OATH-HOTP* (*Open Authentication-*

HMAC Base One Time Password) dengan media *USB device* untuk proses *authentication*, pembahasan mengenai masalah-masalah keamanan pada sistem yang menggunakan *One Time Password* (*OTP*) dan *HMAC-SHA1*.

BAB 5 PENUTUP berisi tentang kesimpulan dari pemanfaatan *One Time Password* (*OTP*) dan algoritma *HMAC-SHA1* pada *USB Device* untuk proses *authentication*.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Hasil dari pembahasan yang telah dilakukan oleh penulis, maka penulis mendapat kesimpulan sebagai berikut :

a. Proses *authentication* yang memanfaatkan *OTP* terdiri dari 3 bagian, yaitu: *credential provisioning*, *password retrieval*, dan *password transport and validation*. *Credential provisioning* merupakan proses yang membantu supaya kunci/*secret* yang digunakan antar *client* dan *server* sama, *password retrieval* merupakan pengambilan *OTP* dari sebuah token, dan *password transport and validation* merupakan proses pentransferan *OTP* ke sebuah *validation server* untuk divalidasi. *Output OTP token* terdiri dari 2 jenis: 6 *digit* atau 8 *digit* angka.
b. Permasalahan keamanan yang kemungkinan terjadi pada sistem yang menggunakan *OATH-HOTP*, terdiri dari: *protocol security*, *user attacks*, dan *device and host security*. Serangan terhadap kekuatan kriptografi yang paling memungkinkan adalah *brute force attack* yang dimana penyerang memasukkan semua kemungkinan angka yang ada, dengan memberikan jangka waktu satu atau beberapa hari setelah beberapa kali gagal dalam pencobaan verifikasi dapat memberikan jangka waktu yang lama bagi penyerang untuk dapat memasukan semua kemungkinan angka yang ada (yang dihasilkan oleh *token*).

5.2 Saran

Hasil dari pembahasan yang telah dilakukan, maka penulis memberikan saran sebagai berikut :

c. Pembahasan dapat dikembangkan lagi dengan membahas *HMAC* yang menggunakan algoritma yang lain dari fungsi *hash seperti*: *MD5*, *SHA-224*, *SHA-256*, *SHA-384*, dan *SHA-512*.

DAFTAR PUSTAKA

Bellare, M., Canetti, R., & Krawczyk, H. (1996). *Message Authentication using Hash Functions-The HMAC Construction.* Dipetik Juli 10, 2013, dari http://charlotte.ucsd.edu/~mihir/papers/hmac-cb.pdf

Chaves, R., Kuzmanov, G., Sousa, L., & Vassiliadis, S. (2006). *Rescheduling for Optimized SHA-1 Calculation.* Dipetik Juli 10, 2013, dari http://link.springer.com/content/pdf/10.1007%2F11818175_36.pdf

Eastlake, D., & Jones, P. (2001, September). *US Secure Hash Algorithm 1 (SHA1).* Dipetik April 30, 2013, dari Internet Engineering Task Force [IETF]: http://tools.ietf.org/pdf/rfc3174.pdf

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering - Design Principles and Practical Applications.* Indianapolis: Wiley Publishing, Inc.

Fouque, P.-A., Leurent, G., Réal, D., & Valette, F. (2009, Juni 16). *Practical Electromagnetic Template Attack on HMAC.* Dipetik Juli 10, 2013, dari IACR: http://www.iacr.org/archive/ches2009/57470064/57470064.pdf

Haller, N., Metz, C., Nesser, P., & Straw, M. (1998). *RFC 2289 - A One-Time Password System.* Dipetik Juni 16, 2013, dari Internet Engineering Task Force [IETF]: http://tools.ietf.org/html/rfc2289

Josefsson, S. (2011, Juni 8). *YubiKey YubiHSM.* Dipetik Mei 5, 2013, dari http://josefsson.org/talks/yubikeyhsm.pdf

Kim, J., Biryukov, A., Preneel, B., & Hong, S. (2006). *On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1*.* Dipetik April 29, 2013, dari http://eprint.iacr.org/2006/187.pdf

M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005, Desember). *RFC 4226 - HOTP: An HMAC-BASED One Time Password Algorithm.* Dipetik Juni 16, 2013, dari Internet Engineering Task Force [IETF]: http://www.openauthentication.org/pdfs/rfc4226.pdf

Muthohar, M. F. (2009). *Studi Penerapan Beberapa Algoritma Kriptografi Pada IPSec.* Dipetik April 29, 2013, dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2008-2009/Makalah1/MakalahIF30581-2009-a062.pdf

National Institute of Standards and Technology [NIST] . (2008, July). *The Keyed-Hash Message Authentication Code (HMAC).* Dipetik Mei 1, 2013, dari csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

National Institute of Standards and Technology [NIST]. (2012, Agustus). *HMAC SHA1.* Dipetik Juli 23, 2013, dari http://csrc.nist.gov/groups/ST/toolkit/documents/Examples/HMAC_SHA1.pdf

National Institute of Standards and Technology [NIST]. (2012, Maret). *Secure Hash Standard (SHS).* Dipetik April 29, 2013, dari http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

National Institute of Standards and Technology [NIST]. (2012, Agustus). *SHA1.* Dipetik Juli 23, 2013, dari http://csrc.nist.gov/groups/ST/toolkit/documents/Examples/SHA1.pdf

Paterson, K. G., & Stebila, D. (2009, September 4). *One-Time Password-Authentication Key Exchange.* Dipetik April 29, 2013, dari eprint.iacr.org/2009/430.pdf

RSA Security. (2005, Februari). *Open Specification Integrate One-Time Passwords with Enterprise Applications.* Dipetik April 29, 2013, dari http://www.rsa.com/rsalabs/otps/datasheets/OTP_WP_0205.pdf

Stamp, M. (2011). *Information Security - Principles and Practice.* San Jose: Wiley.

Yiakoumis, I., Papadonikolakis, M., Michail, H., Kakarountas, A. P., & Goutis, C. E. (2005, November 22-24). Efficient Small-Sized Implementation of the Keyed-Hash Message Authentication Code. *Computer as a Tool, 2005. EUROCON 2005.The International Conference on (Volume:2)* , 1875-1877.

Yubico. (2013, April 18). *The YubiKey Manual.* Dipetik Mei 4, 2013, dari Yubico: http://www.yubico.com/wp-content/uploads/2013/04/YubiKey-Manual-v3_1.pdf

Yubico. (2012, Juli 23). *YubiKey Security Evaluation.* Dipetik Mei 6, 2013, dari Yubico: http://static.yubico.com/var/uploads/pdfs/Security%20Evaluation%202_0_1.pdf