ANALISIS DAN IMPLEMENTASI ALGORITMA SHA-1 DAN SHA-3 PADA SISTEM AUTENTIKASI GARUDA TRAINING COST

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Firlhi Kurniawan
NIM: 135150200111102

PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2017

PENGESAHAN

ANALISIS DAN IMPLEMENTASI ALGORITMA SHA-1 DAN
SHA-3 PADA SISTEM AUTENTIKASI GARUDA TRAINING COST

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Firlhi Kurniawan
NIM: 1351502001111102

Skripsi ini telah diuji dan dinyatakan lulus pada
30 Mei 2017
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Ari Kusyanti, S.T, M.Sc	Heru Nurwarsito, Ir., M.Kom
NIK: 201102 831228 2 001	NIP: 196504021990021001

Mengetahui
Ketua Jurusan Teknik Informatika

Tri Astoto Kurniawan, S.T, M.T, Ph.D
NIP: 19710518 200312 1 001

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 30 Mei 2017

Firlhi Kurniawan

NIM: 135150200111102

KATA PENGANTAR

Puji dan syukur atas kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost". Skrispi ini disusun untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Komputer.

Untuk menyelesaikan penulisan skripsi ini, penulis tidak lepas dari bantuan dari berbagai pihak yang telah banyak memberikan bantuan dan dukungan. Dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Ibu Ari Kusyanti, S.T, M.Sc selaku dosen pembimbing yang telah dengan sabar, tekun, tulus, dan ikhlas meluangkan waktu, tenaga, serta pikiran dalam memberikan arahan, bimbingan, motivasi dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.
2. Bapak Heru Nurwarsito, Ir., M.Kom selaku dosen pembimbing yang telah dengan sabar, tekun, tulus, dan ikhlas meluangkan waktu, tenaga, serta pikiran dalam memberikan arahan, bimbingan, motivasi dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.
3. Orang tua, keluarga, teman-teman dan seluruh orang yang telah banyak membantu dan mendoakan untuk penyelesaian skripsi ini.

Penulis menyadari bahwa dalam penyusunan proposal ini masih banyak terdapat kekurangan, sehingga penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi semua dan berguna untuk pengembangan ilmu pengetahuan.

Malang, 30 Mei 2017

Penulis

firlhik@gmail.com

ABSTRAK

Garuda Training Cost merupakan suatu aplikasi *web* perhitungan biaya pelatihan untuk pilot dan pramugari yang dikembangkan di Garuda Indonesia Training Center. Aplikasi ini menggunakan algoritma *hash function* SHA-1 untuk mengamankan *password* pengguna yang tersimpan di *database*. Tetapi, dikarenakan telah ditemukannya kelemahan dan kolisi pada algoritma ini, maka algoritma ini sudah kurang aman lagi. Maka dari itu, pada penelitian ini, penulis akan menggantikan algoritma SHA-1 tersebut dengan algoritma penerusnya, yaitu SHA-3. Algoritma SHA-3 diimplementasikan pada proses *login*, proses perubahan *password* pengguna dan proses penambahan pengguna. Setelah itu dilakukan pengujian dan analisis untuk mengetahui kinerja dari kedua algoritma tersebut. Ada tiga jenis pengujian yang dilakukan, yang pertama yaitu pengujian *brute-force*, yang kedua pengujian *avalanche effect* dan yang terakhir pengujian waktu pemrosesan. Dari pengujian *brute-force*, algoritma SHA-3 jauh lebih baik dari algoritma SHA-1. Ditunjukkan dengan 30 kali percobaan *brute-force* untuk *password* dengan 10 karakter, *hash* yang dihasilkan SHA-1 membutuhkan waktu rata-rata 14 jam 53 menit dan 51 detik untuk menemukan *plaintext*-nya. Sedangkan *hash* yang dihasilkan SHA-3 membutuhkan waktu rata-rata 4 hari 13 jam 6 menit dan 6 detik untuk menemukan *plaintext*-nya. Untuk pengujian *avalanche effect*, algoritma SHA-1 mendapatkan persentase perubahan sebesar 100% sedangkan SHA-3 mendapatkan 95%. Sedangkan untuk pengujian waktu pemrosesan, SHA-1 lebih baik karena kompleksitas algoritma SHA-3 yang lebih tinggi. Walaupun dua dari tiga pengujian tersebut SHA-1 lebih unggul, bukan berarti SHA-3 tidak lebih baik. Persentase minimum *avalanche effect* untuk sebuah algoritma agar dapat dikatakan baik adalah lebih dari 50%. Sedangkan waktu pemrosesan tersebut masih dalam satuan *millisecond*, sehingga pengguna tidak merasakan dampaknya secara langsung. Kesimpulannya, dari ketiga pengujian tersebut menunjukkan bahwa SHA-3 memiliki ketahanan yang lebih tinggi dari algoritma SHA-1.

Kata Kunci: aplikasi *web*, keamanan *password*, fungsi *hash*, kriptografi, algoritma SHA-1, algoritma SHA-3

ABSTRACT

Garuda Training Cost is a web application for calculating the training costs for pilots and flight attendants developed in Garuda Indonesia Training Center. This application use SHA-1 hash function algorithm to secure user password in database. However, the weakness and colisions have been found in this algorithm, makes this algorithm less secure. Therefore, in this research authors will replace the SHA-1 with the algorithm successor, SHA-3. This algorithm will be implemented in login process, password change process and adding users process. And then both algorithm will be tested and analyzed to determine the performance of the algorithm. There are three types of tests performed. The first is brute-force testing, second is avalanche effect testing and the final test is processing time testing. From the brute-force test result, SHA-3 algorithm much better than SHA-1. From the 30 times testing for 10-character password, the SHA-1 generated hash need average 14 hours 53 minutes and 51 seconds to find the plaintext. While SHA-3 generated hash need average 4 days 13 hours 6 minutes and 6 seconds to find the plaintext. For the avalanche effect testing, SHA-1 algorithm get a percentage change of 100%, while SHA-3 get 95%. For the processing time testing, SHA-1 algorithm is better because of SHA-3 higher complexity. Although two of three test SHA-1 is better, does not mean SHA-3 is not better. Minimum avalanche effect percentage for an algorithm is 50%. And that processing time is still in millisecond unit, so that user do not feel the impact directly. In conclusion, the three these tests show that the SHA-3 has a higher resistance than the algorithm SHA-1.

Keyword: *web application, password security, hash function, cryptography, SHA-1 algorithm, SHA-3 algorithm*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN