ISSN 2087-0256

smatika Jurnal

STIKI Informatika Jurnal

Volume 05, Nomor 02 Tahun 2015

ISSN 2087-0256

smatika Jurnal

STIKI Informatika Jurnal

Volume 05, Nomor 02 Tahun 2015

Lembaga Penelitian & Pengabdian Masyarakat
SEKOLAH TINGGI INFORMATIKA & KOMPUTER INDONESIA

PENGANTAR REDAKSI

STIKI Informatika Jurnal (SMATIKA Jurnal) merupakan jurnal yang diterbitkan oleh Lembaga Penelitian & Pengabdian kepada Masyarakat (LPPM), Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) Malang.

Pada edisi ini, SMATIKA Jurnal menyajikan 14 (*empat belas*) naskah dalam bidang sistem informasi, jaringan, pemrograman web, perangkat bergerak dan sebagainya. Redaksi mengucapkan terima kasih dan selamat kepada Pemakalah yang diterima dan diterbitkan dalam edisi ini, karena telah memberikan kontribusi penting pada pengembangan ilmu dan teknologi.

Pada kesempatan ini, redaksi kembali mengundang dan memberi kesempatan kepada para Peneliti di bidang Teknologi Informasi untuk mempublikasikan hasil-hasil penelitiannya melalui jurnal ini. Bagi para pembaca yang berminat, Redaksi memberi kesempatan untuk berlangganan.

Akhirnya Redaksi berharap semoga artikel-artikel dalam jurnal ini bermanfaat bagi para pembaca khususnya dan bagi perkembangan ilmu dan teknologi di bidang Teknologi Informasi pada umumnya.

REDAKSI

ISSN 2087-0256

smatika Jurnal

STIKI Informatika Jurnal

Volume 05, Nomor 02 Tahun 2015

SEKRETARIAT
Lembaga Penelitian & Pengabdian kepada Masyarakat
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI)
Malang
smatika Jurnal
Jl. Raya Tidar 100 Malang 65146
Tel. +62-341 560823
Fax. +62-341 562525
Website: jurnal.stiki.ac.id
E-mail: lppm@stiki.ac.id

ISSN 2087-0256
Volume 05, Nomor 02 Tahun 2015

DAFTAR ISI

Undangan Makalah

smatika Jurnal Volume 06, Nomor 01 Tahun 2016

Implementasi Teknik Kriptografi Stream Cipher Salsa20 Untuk Pengamanan Basis Data

Paulus Lucky Tirma Irawan
Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Ma Chung
Villa Puncak Tidar N-01, Malang, 65151, Indonesia
E-mail: paulus.lucky@machung.ac.id

ABSTRAK

Dari teknologi surat elektronik (e-mail), komunikasi selular, keamanan akses laman web, hingga sistem pembayaran online, kriptologi memegang peranan penting. Berdasarkan penelitian, ditemukan fakta bahwa telah terjadi peningkatan ancaman terhadap keamanan data secara signifikan dalam beberapa tahun terakhir. Beberapa literatur pustaka menjelaskan secara rinci bahwa pencurian data atau informasi masih menjadi kasus dengan total persentase kejadian yang paling tinggi saat ini.
Tujuan dari penelitian ini adalah meningkatkan keamanan data pada basis data MySQL menggunakan teknik kriptografi stream cipher Salsa20. Algoritma ini termasuk ke dalam salah satu kandidat algoritma kriptografi stream cipher terbaik menurut eSTREAM portfolio tahun 2012. Tahapan penelitian diawali dengan desain skema proses enkripsi-dekripsi data di sisi client-server, pembuatan modul fungsi kriptografi Salsa20 yang dilanjutkan dengan tahapan pengujian.
Berdasarkan penelitian yang sudah dilakukan, implementasi teknik kriptografi Salsa20 dapat menjadi sebuah solusi alternatif untuk meningkatkan keamanan data dengan memberikan sebuah layer keamanan pada data yang terdapat di dalam basis data MySQL melalui proses enkripsi. Pengembalian data dari basis data MySQL hanya dapat dilakukan jika data yang sudah terenkripsi sebelumnya di dekripsi menggunakan parameter masukan key yang sama. Proses dekripsi yang dilakukan dengan menggunakan key yang salah hanya akan mengembalikan susunan data yang tidak memiliki makna bagi pengguna.

Kata Kunci : *stream cipher, enkripsi, dekripsi, salsa20*

1. PENDAHULUAN

Latar Belakang

Dalam sebuah laporan yang dirilis oleh sebuah badan pemerintahan *California Department of Justice: Privacy Enforcement and Protection Unit* tahun 2014, diketahui bahwa ancaman keamanan data terus mengalami peningkatan dibandingkan data pada tahun 2012 lalu yang melibatkan hampir 41 juta data transaksi pembayaran. Hal ini tidak jauh berbeda dengan temuan yang dipaparkan oleh Symantec dalam *Symantec Internet Security Threat Report 2014 Volume 19: Mobile Threat Classifications*. Dalam laporannya dikemukakan bahwa ancaman terhadap pencurian data masih menjadi kasus dengan total persentase tertinggi dibandingkan empat kategori ancaman lainnya, seperti pengiriman konten, adware, konfigurasi ulang perangkat, serta ancaman-ancaman konvensional lainnya. Aksi peretasan yang dilakukan oleh kelompok peretas yang menamai dirinya Guardian of Peace terhadap SONY Pictures Entertainment baru-baru ini dapat menjadi salah satu contoh bagaimana pentingnya menyajikan sebuah keamanan data yang baik (Kompas, diakses 3 Desember 2014).

Untuk dapat meningkatkan keamanan data dapat digunakan teknik-teknik keamanan data seperti kriptografi dan steganografi. Kedua teknik ini memiliki proses kerja yang berbeda dalam melakukan pengamanan data. Kriptografi bekerja dengan melakukan proses pengacakan data terhadap pesan data asli (*plain-text*) sehingga data yang asli tidak dapat dibaca oleh pihak yang tidak berkepentingan tanpa mengetahui kunci khusus (*key*) untuk membaca pesan (*cipher-text*) tersebut. Sementara steganografi bekerja dengan menyisipkan pesan data asli (*secret-message*) ke dalam sebuah data lainnya yang bertindak sebagai media (*cover image/vessel image*) sehingga pihak yang tidak berkepentingan tidak menyadari kehadiran dari pesan yang ada dibalik data media tersebut.

Dalam penelitian ini akan digunakan teknik kriptografi *stream cipher* Salsa20 yang diciptakan pada tahun 2005 oleh Daniel J. Bernstein. Teknik kriptografi Salsa20

termasuk ke dalam salah satu kandidat eSTREAM Project. eSTREAM Project bertujuan untuk melakukan pengembangan terhadap algoritma kriptografi berbasis *stream cipher*. Proyek eSTREAM ini berada di bawah pengawasan organisasi *European Network of Excellence in Cryptography* (ECRPYT). Penerapan teknik kriptografi Salsa20 dapat memberikan lapisan keamanan terhadap data atau informasi pengguna yang terdapat di dalam sebuah server manajemen basis data (DBMS).

Rumusan Masalah

Dengan mengkaji latar belakang yang ada, maka permasalahan yang diangkat pada penelitian ini adalah "Bagaimana mendesain dan melakukan implementasi teknik kriptografi *stream cipher* Salsa20 untuk meningkatkan keamanan data pada basis data MySQL".

1. TINJAUAN PUSTAKA

Kriptografi

Berdasarkan proses enkripsi dan dekripsi yang dikenakan pada pesan yang akan dikirimkan, kriptografi dapat dikelompokkan kembali ke dalam dua bagian (Munir, 2006), yakni:

a. Cipher blok (*block cipher*)
   Kriptografi cipher blok menerima masukan dalam bentuk sekumpulan blok bit dengan panjang tertentu. Dengan algoritma ini, blok plain teks yang sama akan dienkripsi menjadi blok cipher teks yang sama bila menggnakan kunci yang sama juga.
b. Cipher aliran (*stream cipher*)
   Kriptografi cipher aliran menerima parameter masukan dalam bentuk aliran bit. Proses enkripsi dan dekripsinya dilakukan pada aliran bit dengan memproses bit satu per satu. Secara umum stream cipher membangkitkan aliran kunci dari kunci yang dimasukkan oleh pengguna. Ketika aliran kunci telah dibangkitkan, maka proses enkripsi dan dekripsi dilakukan melalui operasi XOR antara bit aliran kunci dengan bit plaintext atau ciphertext.

Keamanan kriptografi cipher aliran sangat bergantung pada proses pembangkitan aliran kunci. Apabila dalam proses pembangkit aliran kunci, aliran kunci yang dihasilkan bernilai nol pada keseluruhan bit nya, maka cipher teks yang dihasilkan akan sama seperti plain teks, yang berakibat pada proses enkripsi menjadi sia-sia. Semakin acak keluaran yang dihasilkan dari proses pembangkit aliran kunci, maka cipher-text yang dihasilkan juga akan semakin sulit dipecahkan.

Salsa20

Salsa20 merupakan algoritma kriptografi berbasis cipher aliran (*stream cipher*). Algoritma kriptografi ini dikembangkan oleh Daniel J. Bernstein pada tahun 2005 dan termasuk ke dalam salah satu kandidat eSTREAM Project (eCRYPT, diakses Januari 2014). eSTREAM Project bertujuan untuk melakukan pengembangan terhadap algoritma kriptografi berbasis cipher aliran. Proyek eSTREAM ini berada di bawah pengawasan organisasi *European Network of Excellence in Cryptography* (ECRPYT).

Secara umum, algoritma kriptografi Salsa20 membangkitkan aliran kunci dari kunci masukan, kemudian melakukan operasi XOR antara aliran kunci dengan cipher teks atau plain teks. Algoritma Salsa20 menerima masukan berupa 32 bytes key, 8 byte nonce (maksimum), 8 byte block counter (maksimum). Setelah dilakukan proses pembangikitan aliran kunci kemudian dilakukan operasi XOR antara aliran kunci dan plain teks. Besar aliran kunci yang dihasilkan adalah 64 byte. Salsa20 membangkitkan aliran kunci dengan cara sebagai berikut:

a. Salsa20 membangun array yang berisi 16 words. Tiap words berukuran 32 bit. 16 words tersebut adalah: constant word 0x61707865, 4 buah key word pertama,7 constant word 0x3320646e, 2 nonce word, 2 block word, constant word 0x79622d32, sisa 4 key word, dan constant word 0x6b206574. Misalkan: input key (1, 2, 3, 4, 5, .. , 32), nonce (3, 1, 4, 1, 5, 9, 2, 6), dan block 7.
b. Salsa20 kemudian memodifikasi setiap baris word di bawah garis diagonal, kemudian melakukan operasi pertambahan antara garis diagonal dengan word di atas garis diagonal, kemudian melakukan operasi rotasi sebanyak 7 bit ke arah kiri, dan melakukan operasi XOR dengan word di bawah garis diagonal.
c. Salsa20 kemudian memodifikasi baris kedua di bawah garis diagonal, kemudian melakukan operasi penambahan antara word di bawah garis diagonal dengan garis diagonal, kemudian melakukan operasi rotasi sebanyak 9 bit ke arah kiri,

dan melakukan operasi XOR dengan word baris kedua di bawah garis diagonal.
d. Salsa 20 kemudian melanjutkan modifikasi yang sama di setiap kolom, baris berikutnya. Namun pada tahapan ini diikuti dengan operasi rotasi sebanyak 13 bit ke arah kiri.
e. Salsa20 melanjutkan modifikasi yang sama di setiap kolom, baris berikutnya. Pada proses ini terjadi operasi rotasi sebanyak 18 bit ke arah kiri.
f. Salsa20 kemudian melakukan operasi transpose pada larik yang telah terbentuk sebelumnya.
g. Ulangi langkah 1 s.d. 6 sebanyak 19 kali.
h. Setelah iterasi ke-20, Hasil akhir dari larik ini kemudian akan ditambahkan ke larik awal untuk mendapatkan 64 bytes blok keluaran.

2. METODOLOGI PENELITIAN

Perancangan perangkat lunak yang menerapkan teknik kriptografi stream cipher Salsa20 ini dilakukan dengan mempersiapkan beberapa tahapan yang harus dilalui, meliputi:

Analisa Kebutuhan

Tahapan penelitian diawali dengan analisa kebutuhan untuk mengetahui komponen-komponen yang harus disiapkan untuk menunjang pekerjaan pada tahapan selanjutnya, meliputi kebutuhan perangkat lunak, perangkat keras, serta kebutuhan pengguna yang menjadi fokus pencapaian penelitian ini.

Untuk komponen perangkat lunak nantinya akan dibagi ke dalam dua kategori, yakni kompoenen perangkat lunak yang dibutuhkan untuk proses pengembangan serta komponen perangkat lunak yang dibutuhkan untuk proses penggunan/uji coba di sisi end-user. Adapun perangkat pengembang (IDE) yang akan digunakan yakni editor teks, bahasa skrip HTML&Javascript, bahasa pemrograman client-side PHP, perangkat lunak server manajemen basis data (DBMS) MySQL, peramban Chrome untuk pengujian skrip, serta sebuah perangkat tambahan XAMPP untuk pengujian lokal (localhost) untuk mempercepat proses pengembangan perangkat lunak. Untuk keperluan pengujian hanya diperlukan peramban dengan koneksi Internet yang memadai.

Sementara untuk kebutuhan perangkat keras tidak membutuhkan spesifikasi khusus di sisi klien, namun untuk pengujian aplikasi luar lokal (Internet) nantinya akan dibutuhkan sebuah server untuk menampung skrip aplikasi yang dikembangkan. Hal ini diperlukan untuk dapat mengetahui secara real-time performansi dari implementasi teknik kriptografi Salsa20 dalam proses enkripsi-dekripsi data pada basis data dengan model arsitektur multi-tier (n-tier).
Pengembangan dilakukan dengan memperhatikan hasil analisa kebutuhan pengguna (analisa masalah), yakni bagaimana menyediakan sebuah modul kriptografi (enkripsi/dekripsi) stream cipher Salsa20 untuk pengamanan basis data MySQL.

Studi Literatur

Pada tahapan ini akan dilakukan pencarian data terhadap penelitian-penelitian yang sudah pernah dilakukan terkait dengan konsep pengamanan data pada basis data, termasuk di dalamnya alur kerja dari pada teknik kriptografi Salsa20 itu sendiri. Dengan begini diharapkan proses desain sistem yang menggambarkan skema proses enkripsi-dekripsi data pada basis data dapat dilakukan dengan lebih terarah dan memiliki landasan yang kuat.

Desain Sistem

Pada tahapan sistem akan dihasilkan sebuah skema yang menjelaskan alur kerja sistem secara umum dan spesifik. Skema alur kerja ini akan menjadi cetak biru dalam proses pengembangan aplikasi selanjutnya. Skema alur kerja umum akan menjelaskan secara garis besar proses kerja sistem yang dirancang mulai dari proses permintaan data ke server manajemen basis data (*data request*) hingga respon server (*data respond*) kepada requester, dalam hal ini adalah peramban. Sementara skema alur kerja spesifik lebih menekankan pada cara kerja Salsa20 dalam melakukan proses enkripsi-dekripsi data yang terdapat di dalam basis data.

Pengembangan Aplikasi

Luaran dari tahapan ini adalah sebuah aplikasi yang menerapkan skema pengamanan basis data menggunakan teknik kriptografi stream cipher Salsa20 dengan luaran utama berupa modul yang berisi fungsi-fungsi yang dapat digunakan sebagai library eksternal untuk fungsi enkripsi-dekripsi data pada basis data MySQL.

Pengujian

Pada tahapan ini akan dilakukan serangkaian pengujian untuk mengetahui konsistensi dari setiap luaran fungsi (*return value*) yang sudah dikembangkan. Pengujian dilakukan untuk mengetahui keberhasilan proses enkripsi dan dekripsi data pada saat proses pengiriman data ke klien (*Unit Testing*).

Pelaporan

Tahapan ini merupakan tahapan akhir yang bertugas mendokumentasikan proses penelitian yang sudah dilakukan mulai dari tahapan awal analisa kebutuhan hingga tahapan pengujian. Luaran dari pada tahapan ini adalah sebuah laporan kegiatan penelitian yang komprehensif serta dokumentasi proyek yang menjabarkan secara detil fungsi-fungsi yang sudah dihasilkan dalam modul enkripsi-dekripsi Salsa20.

3. HASIL DAN PEMBAHASAN

Dokumentasi alir kerja teknik kriptografi *stream cipher* Salsa20 berisi tentang deskripsi rinci alir kerja dari teknik kriptografi cipher aliran Salsa20 yang menjadi fokus utama penelitian ini. Dokumentasi ini menjabarkan secara rinci 2 proses utama yang dilakukan di dalam teknik kriptografi Salsa20, yakni proses enkripsi data (*plaintext to ciphertext*) dan proses dekripsi data (*ciphertext to plaintext*).

Secara umum alir kerja teknik kriptografi Salsa20 dapat dilihat pada tabel IPO (Input-Proses-Output) berikut.

Tabel 1. Diagram IPO

Input	Proses	Output
inisialisasi - Data pesan (*plain-text*) - key (16 karakter) - param IV	Algoritma enkripsi / dekripsi Kriptografi cipher aliran Salsa20	Data terenkripsi (*cipher-text*)

Dari tabel diagram IPO tersebut, dapat diketahui bahwa teknik kriptografi Salsa20 bekerja diawali dengan proses inisialisasi untuk menentukan parameter masukan meliputi data pesan, komponen key sepanjang 16 karakter dan sebuah parameter IV. Bagian proses menjelaskan bagaimana tahapan di dalam Salsa20 itu bekerja sebelum menghasilkan data terenkripsi (*cipher-text*) pada proses enkripsi atau data plain (*plain-text*) pada saat proses dekripsi. Sementara keluaran dari pada implementasi teknik kriptografi salsa20 ini adalah sebuah data terenkripsi (*cipher-text*) yang akan disimpan ke dalam basis data MySQL.

Pembuatan modul fungsi kriptografi Salsa20 mengikuti prinsip kerja yang telah dituangkan oleh Daniel J. Bernstein pada spesifikasi Salsa20. Modul fungsi kriptografi Salsa20 menghasilkan dua fungsi utama, yakni fungsi enkripsi salsa20_encrypt($data, $key, $iv) dan fungsi dekripsi yang digunakan untuk mengambalikan data terenkripsi melalui fungsi salsa20_decrypt($data, $key, $iv).

Setelah dibentuk modul fungsi kriptografi Salsa20, maka tahapan selanjutnya adalah melakukan pengujian terhadap basis data MySQL. Dalam penelitian ini, pengujian dilakukan pada dua proses utama, yakni proses enkripsi data untuk menghasilkan data terenkripsi yang akan disimpan di dalam basis data MySQL serta proses dekripsi untuk mendapatkan bentuk asli (*plain-text*) dari basis data tersebut sehingga memiliki arti bagi penggunanya.

Berikut ini adalah hasil pengujian terhadap data *plain-text* untaian kata “UNIVERSITAS MA CHUNG”.

Tabel 2. Hasil Enkripsi Salsa20

Plain-text	UNIVERSITAS MA CHUNG
Cipher-text	c  -    ^    8  !{ 

Sementara pada proses selanjutnya, yakni proses pemanggilan data dari basis data (proses dekripsi), urutan proses yang berjalan tidak jauh berbeda dengan proses enkripsi, hanya saja fungsi yang dipanggil adalah salsa20_decrypt() yang tidak lain berisi fungsi enkripsi salsa20_encrypt itu sendiri. Dalam spesifikasi Salsa20 diketahui bahwa proses dekripsi tidak lain adalah proses enkripsi salsa20, hanya saja parameter data masukan yang digunakan adalah parameter data masukan yang sudah dienkripsi dengan kunci dan parameter IV yang sama.

Berikut ini adalah hasil pengujian terhadap data *cipher-text* “c  -   ^   8!{”.

Tabel 3. Hasil Dekripsi Salsa20

Cipher-text	c  -    ^    8  !{ 
Plain-text	UNIVERSITAS MA CHUNG

Sementara tabel 4 berikut ini akan memberikan ilustrasi jika proses dekripsi

tidak dilakukan dengan menggunakan parameter kunci dan IV yang sama dengan proses enkripsi sebelumnya.

Tabel 4. Hasil Dekripsi Salsa20

Cipher-text	c�-� ��^ �� �8�!{
Plain-text	c�-� ��^ �� �8�!{

Dapat dilihat bahwa hasil keluaran fungsi dekripsi akan memberikan hasil yang tidak bermakna jika parameter kunci dan IV yang digunakan tidak sama dengan parameter masukan pada proses enkripsi sebelumnya.

4. KESIMPULAN

Implementasi teknik kriptografi *stream cipher* Salsa20 dapat digunakan untuk memberikan peningkatan keamanan data melalui proses enkripsi-dekripsi sebelum data disimpan di dalam sebuah basis data. Pengembalian data dari basis data MySQL hanya dapat dilakukan jika data yang sudah terenkripsi sebelumnya di dekripsi menggunakan parameter masukan key yang sama. Proses dekripsi yang dilakukan dengan menggunakan key yang salah hanya akan mengembalikan susunan data yang tidak memiliki makna bagi pengguna. Hal ini tentunya dapat menjadi alternatif solusi untuk pengamanan data pada basis data dari pihak yang tidak berkepentingan.

5. REFERENSI

[1]. Bernstein, Daniel J. (10 Januari2014). Salsa20 Spesification. Tersedia: http://cr.yp.to/snuffle/spec.pdf

[2]. eCRYPT. (12 Oktober 2012). D. SYM. 10 The eSTREAM Portfolio in 2012 [Online].

[3]. Tersedia:http://www.ecrypt.eu.org/documents/D.SYM.10-v1.pdf

[4]. Munir, Rinaldi. Kriptografi. Bandung: Informatika, 2006

[5]. Symantec. Mobile Threat Classifications. Symantec Internet Security Threat Report Vol. 19. Agustus, 2014

[6]. [1] Webroot. (4 Februari 2014). Webroot Mobile Threat Report: An Overview of The Risks and Trends of The Mobile Space [Online]

[7]. Tersedia:http://www.webroot.com/shared/pdf/WR_MobileThreatReport_v4_20140218101834_565288.pdf