PENGGUNAAN ALGORITMA SHA-512 UNTUK MENJAMIN INTEGRITAS DAN KEOTENTIKAN PESAN PADA INTRANET

Megah Mulya
Universitas Sriwijaya, Palembang
megahmulya@yahoo.com

ABSTRACT

Data security has become a basic need in every organization or company. Generally, to support their businesses, organizations or companies need a mean of communication between the branch offices so that intranet is needed. Basically, intranet is a local network and internet is an open network and has not a security mechanism on its protocol (TCP/IP). A security mechanism which guarantees command integrity and authenticity is needed. The selected message security mechanism which uses the cryptography technique using SHA-512 is implemented to guarantee data integrity and authenticity. The literature study conducted includes kind of attack probably happening, algorithm strength and the authentication scheme that is appropriate to be used with intranet environment. From this study, it is concluded that SHA-512 is reliable and can be used to guarantee the data integrity and authenticity which is transmitted to the intranet by using common password between sender and receiver.

Keywords: *Authenticity, Data Integrity, SHA-512, Intranet*

1. Pendahuluan

Keamanan data telah menjadi kebutuhan pokok di hampir setiap organissai/perusahaan. Untuk menunjang bisnisnya organisasi/ perusahaan umumnya memerlukan komunikasi antar kantor cabang atau dengan pihak lain. Oleh karena itu dibutuhkan suatu mekanisme yang menjamin keaslian/keotentikan data yang ditransmisikan melalui media jaringan. Teknik kriptografi telah banyak digunakan untuk keperluan pengamanan data terutama data yang ditransmisikan melalui jaringan komputer. Salah satu kebutuhan keamanan data adalah otentikasi atau jaminan keaslian data. Yang dimaksud jaminan keaslian data adalah kepastian bahwa data yang ditransmisikan melalui jaringan komputer yang diterima oleh pihak penerima adalah benar data yang dikirimkan oleh pihak pengirim yang dikehendaki pihak penerima.

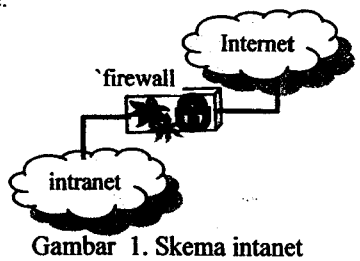
Penelitian ini mempunyai tujuan untuk melakukan kajian kekuatan algoritma SHA-512 jika digunakan untuk menjamin integritas dan keotentikan pesan, dan melakukan kajian skema yang cocok untuk menjaga integritas dan keotentikan pesan yang ditransmisikan di dalam lingkungan intranet. Permasalahan yang akan dipecahkan di dalam penelitian ini adalah bagaimana kekuatan SHA-512 cukup kuat untuk digunakan di dalam menjamin integritas dan keotentikan pesan dan bagaimana skema keamanan yang sesuai diterapkan dengan karakteristik intranet.

2. Landasan Teori

2.1 Intranet

Intranet sebenarnya adalah skala kecil. *Intranet* beroperasi sebagai *internetwork* lokal. *Intranet* terhubung dengan *Internet* melalui *firewall* yang berperan sebagai penyaring lalu-lintas data. Penyaringan lalu-lintas data tersebut menyangkut apa saja yang boleh diakses atau apa saja yang tidak boleh diakses dari *Intranet* maupun dari *Internet*.

Untuk menghubungkan cabang-cabang dalam organisasi dibutuhkan *internetwork*. Untuk membangun *internetwork* solusi paling menguntungkan adalah dengan konsep *intranet* yang memanfaatkan keberadaan Internet dengan protokolnya TCP/IP. Keuntungan itu di antaranya berkaitan dengan kompatibilitas, harga lebih murah dibanding jenis network yang lain (misalnya dengan Novell Netware), kemudahan, dan skalabilitas. Gambar 1 memberikan ilustrasi tentang *intranet* yang memanfaatkan *Internet*.



Gambar 1. Skema intanet

2.2 Serangan Terhadap Transmisi Data

Serangan terhadap data yang ditransmisikan melalui jaringan komputer dikelompokkan dalam dua kategori[6] yaitu:

(1) Serangan pasif (*passive attack*): penyerang tidak terlibat aktif dalam pertukaran informasi. Tetapi hanya menguping atau memonitor transmisi.
(2) Serangan aktif (*active attack*): penyerang aktif terlibat dalam pertukaran informasi dengan cara melakukan interupsi untuk melakukan perubahan atau penggandaan pesan-pesan dalam pertukaran informasi.

Kedua jenis serangan tersebut dapat dilakukan dengan berbagai cara seperti terlihat pada Gambar 2, yaitu[6]:

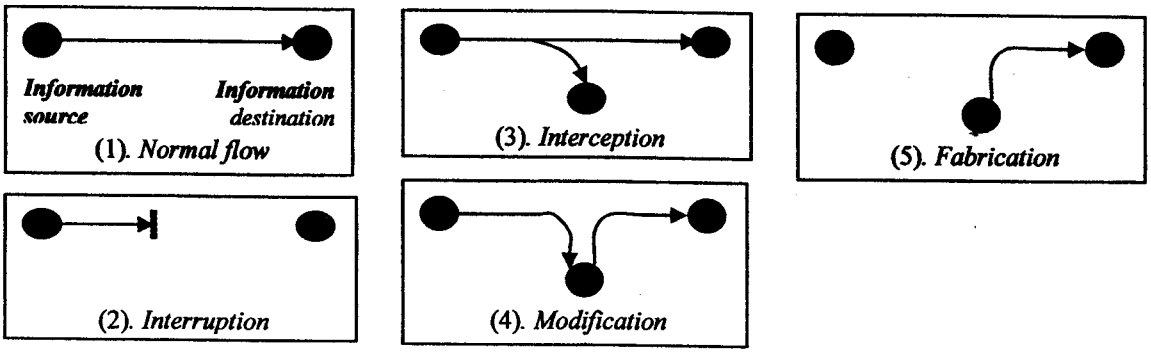
(1). *Interruption*: serangan yang mengakibatkan asset sistem rusak atau tidak dapat digunakan (serangan *availability*)

(2). *Interception*: serangan pihak yang tidak memiliki hak agar dapat mengakses asset dalam sistem (serangan *privacy*)

(3). *Modification:* serangan pihak yang tidak memiliki hak agar dapat merubah data (serangan *integrity*).

(4). *Fabrication*: pihak yang tidak memiliki hak memalsukan suatu obyek tertentu di dalam sistem (serangan *authenticity*).

Skenario dari serangan-serangan tersebut dapat dijelaskan dengan skema sebagai berikut:



Gambar 2. Skenario Serangan Terhadap Keamanan Data

2.3 Pelayanan Keamanan Data

Teknik kriptografi dapat digunakan untuk memberikan berbagai jenis pelayanan keamanan data di antaranya adalah:

(1). Privasi/kerahasiaan (*confidentiality*): informasi yang ditransmisikan hanya boleh diakses oleh sekelompok pengguna yang berhak.

(2). Otentikasi (*authentication*): masalah keaslian pesan berkaitan dengan keutuhan pesan (*data integrity)* dan apakah pihak yang diajak berkomunikasi adalah benar-benar pihak yang dikehendaki

(3). Integritas (*integrity*): pesan yang diterima oleh penerima tidak lagi seperti yang pertama kali dikirim oleh pengirim, akibat disadap dan dimodifikasi oleh penyerang (*attacker*).

(4). Nir-penolakan (*nonrepudiation*): pertukaran informasi tanpa bertemu muka secara langsung dapat menimbulkan pembantahan atas pesan yang pernah dikirim.

(5). Kontrol akses (*access control*): pembatasan dan pemantauan akses ke *host* sistem dan aplikasi yang menggunakan media komunikasi.

(6). Ketersediaan (*availablity*): serangan dapat mengakibatkan terhalangnya sumber daya untuk diakses

2.4 Algoritma SHA-512

Algoritma SHA-512 termasuk jenis fungsi *hash* yang merupakan pengembangan dari algoritma SHA-1. Fungsi *hash* memetakan pesan M dengan panjang berapapun menjadi nilai hash h dengan panjang tetap (tertentu, tergantung algoritmanya). Untuk algoritma SHA-512 panjang nilai *hash* yang dihasilkan adalah 512 bit. Fungsi *hash* yang menghasilkan keluaran dengan ukuran yang kecil mudah diserang oleh *birthday attact*[4]. Serangan ini dilakukan dengan cara mendapatkan dua pesan secara acak yang memiliki nilai *hash* h sama. SHA-512 sebagai fungsi hash mempunyai sifat-sifat sebagai berikut:

(1). h mudah dihitung bila diberikan M.
Sifat ini merupakan keharusan, karena jika h sukar dihitung, maka fungsi hash tersebut tidak dapat digunakan.

(2). M tidak dapat dihitung jika hanya diketahui h.
Sifat ini disebut juga *one-way function*, atau mudah untuk menghitung h dan sukar untuk dikembalikan ke M semula. Sifat ini sangat penting dalam teknik kriptografi, karena jika tanpa sifat tersebut maka penyerang dapat menemukan nilai M dengan mengetahui nilai *hash*-nya h.

(3). Tidak mungkin dicari M dan M' sedemikian sehingga H(M)=H(M').
Sifat ini disebut juga *collision free*. Sifat ini mencegah kemungkinan pemalsuan.

2.5 Otentikasi dengan Fungsi *Hash*.

Fungsi *hash* (H) menyediakan otentikasi pesan. Terdapat beberapa skema untuk keperluan otentikasi pesan yang dikirim dari pengirim A dan diterima oleh penerima B. Pada umumnya kebutuhan otentikasi dikaitkan dengan upaya privasi. Beberapa skenario otentikasi dapat dijelaskan sebagai berikut[6]:

(a) Pesan digabung dengan kode *hash* kemudian dienkripsi dengan kriptografi kunci simetri. Cara ini dapat dilakukan karena A dan B memiliki kunci simetri bersama, sehingga pesan pasti bersumber dari A dan tidak mungkin digantikan pihak lain. Dalam cara ini kode *hash* menyediakan otentikasi sedangkan enkripsi menyediakan privasi.

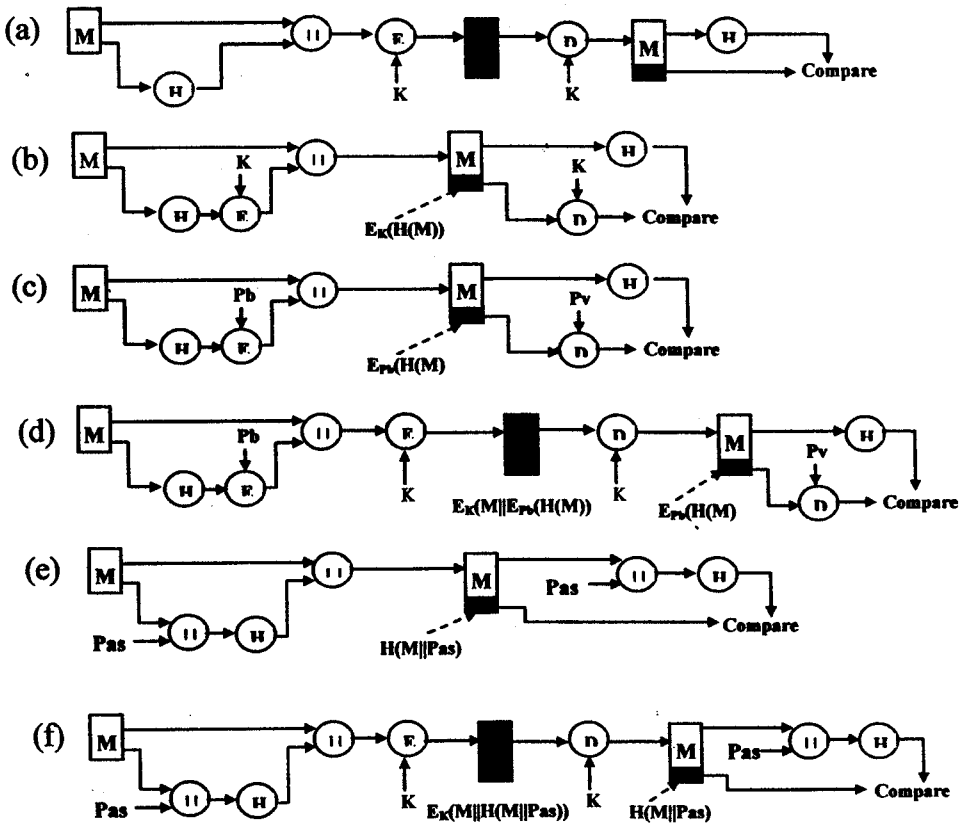
(b) Hanya kode *hash* yang dienkripsi dengan kriptografi kunci simetri. Dengan sekema ini beban proses pada aplikasi dapat dikurangi. Teknik ini hanya menyediakan otentikasi tanpa privasi. E_K (H(M)) merupakan fungsi pesan dengan panjang variable dan kunci rahasia K. Ini menghasilkan output dengan ukuran tetap yang aman untuk melawan penyerang yang tidak mengetahui kunci K. Hanya kode *hash* yang dienkripsi dengan kriptografi kun

publik menggunakan kunci private Pv pengirim (A). Skema ini selain menyediakan otentikasi juga menyediakan *digital signature*, karena hanya A yang dapat menghasilkan kode *hash* yang terenkripsi. Teknik ini merupakan prinsip dari *digital signature*.

Jika kebutuhan privasi sama pentingnya dengan otentikasi maka pesan beserta kode *hash* yang telah dienkripsi menggunakan kunci privat Pv dengan kriptografi kunci publik, dienkripsi lagi dengan kriptografi kunci simetri menggunakan kunci rahasia K.

) Teknik ini menggunakan fungsi *hash* tetapi tidak menggunakan enkripsi dalam tujuan otentikasi pesan. Pada teknik ini diasumsikan bahwa kedua pihak yang berkomunikasi memiliki password (Pas) rahasia yang dipakai bersama. A menghitung nilai has terhadap pesan M yang digabung dengan *password*. Hasilnya digabung lagi dengan M. Karena B juga mengetahui *password*, maka dia juga dapat menghitung nilai *hash* sebagaimana yang dilakukan A. Karena nilai rahasia *password* itu sendiri tidak ikut dikirimkan, maka penyerang tidak dapat merubah pesan yang disadapnya.

ambar berikut ini menjelaskan skema beberapa skenario otentikasi yang telah diuraikan di atas.



Gambar 3. Prinsip Dasar Penggunaan Fungsi *Hash* Untuk Otentikasi Pesan Dalam Transmisi Data

Metodologi Penelitian

etodologi yang digunakan dalam penelitian ini adalah sebagai berikut:

Melakukan kajian jenis serangan yang mungkin terjadi terhadap pesan yang ditransmisikan di dalam lingkungan intranet.

Melakukan kajian terhadap algoritma SHA-512 dari sisi kekuatan dan kecepatan relatif tarhadap algoritma lain yang populer.

Melakukan kajian skema penjaminan integrasi dan otentikasi pesan yang sesuai dengan lingkungan intranet.

Pembahasan

Analisis SHA-512 untuk Menjamin Integritas dan Keotentikan Pesan dalam *Intranet*

laupun di dalam intranet telah ada suatu mekanisme pengamanan data (misalnya *firewall* atau yang lain) tetapi tetap k mencukupi. Pada prinsipnya tidak ada suatu mekanisme keamanan yang benar-benar seratus persen menjamin iruh pelayanan keamanan (*security service*), atau dapat dikatakan tidak ada mekanisme keamanan yang sempurna. g ada hanya mempersulit serangan atau meminimalkan peluang terjadinya serangan[2]. Dengan demikian dibutuhkan anisme pangamanan yang lain yang dapat saling memperkuat.

4.1.1 Jenis Serangan Yang Mungkin Terjadi

Berdasarkan uraian pada bagian 3 di atas tentang jenis-jenis serangan terhadap data yang ditransmisikan dalam jaring maka serangan yang mengancam integritas dan keotentikan pesan adalah jenis serangan aktif (*active attack*) dengan c *Modification* dan *Fabrication*. Setiap pesan dari pengirim yang ditransmisikan seharusnya telah dienkripsi sehing sudah terjamin privasinya. Tetapi dengan serangan aktif tersebut pesan dapat rusak atapun berubah. Sehingga sa dilakukan dekripsi oleh pihak penerima akan menhasilkan pesan tidak bermakna atau dekripsi gagal.

4.1.2 Kehandalan Algoritama SHA-512

Algoritma SHA-512 termasuk fungsi *hash* yang meghasilkan nilai *hash* terpanjang yaitu 512 bit. Dengan demiki berdasarkan uraian pada bagian 2 tentang algoritma SHA-512, algoritma ini akan lebih tahan terhadap serangan *birthd attack* dibanding fungsi *hash* yang lain. SHA-512 termasuk fungsi *hash* merupakan pengembangan dari SHA-1 yan merupakan perbaikan (berbasis) dari MD4[5], karena SHA-512 diketahui dapat dipatahkan oleh *cryptanalyst*. Sedangka MD4 sudah lama diketahui dapat dipatahkan oleh *cryptanalyst* sebelum SHA-1[4]. Beberapa fungsi *hash* yang merupaka perbaikan dari MD4 dapat dilihat pada Tabel 1. Dari tabel tersebut terlihat panjang nilai *hash* dari algoritma SHA-51 termasuk terpanjang disamping algoritma Whirlpool.

Tabel 1. Panjang Nilai *Hash* Fungsi *Hash*[2,7]

Fungsi Hash	Panjang Nilai Hash (bit)
MD2	128
MD4	128
MD5	128
RIPEMD	128
RIPEMD-128/256	128/256
RIPEMD-160/320	160/320
SHA-0	160
SHA-1	160
SHA-256/224	256/224
SHA-512/384	512/384
TIGER(2)-192/160/128	192/160/128
WHIRLPOOL	512

Selain pertimbangan kekuatan algoritma, pertimbangan lain adalah kecepatan. Kecepatan beberapa algoritma kunci simetri dan fungsi hash dapat dilihat pada Tabel 2.

Tabel 2. Kecepatan Beberapa Fungsi Hash[1]

Fungsi Hash/Algoritma Kunci Simetri	MiByte/second
CRC32	253
Adler	920
MD5	255
SHA-1	153
SHA-256	111
SHA-512	99
Tiger	214
Whirlpool	57
RIPEMD-160	106
RIPEMD-320	110
RIPEMD-128	153
RIPEMD-256	158
DES/CTR	32
Blowfish/CTR	58
IDEA/CTR	35
RC5(r=16)	75

Fungsi *hash* pada umumnya digunakan bersama-sama dengan algoritma kunci simetri atau algoritma kunci pub Algoritma kunci simetri diketahui sangat cepat dibandingkan dengan algoritma kunci publik hingga mencapai 1000 lebih cepat[5]. Oleh karena itu untuk mencapai performansi yang baik pemilihan fungsi *hash* adalah cukup masuk a jika berdasarkan perbandingan kecepatannya terhadap algoritma kunci simetri. Dari Tabel 2 dapat disimpulkan se fungsi *hash* memiliki kecepatan melebihi algoritma kriptografi kunci simetri. SHA-512 memiliki kecepatan MiBute/second didalam prosesnya yang masih masih melebihi kecepatan algoritma kunci simetri RC5 yang ter dengan 75 MiByte/second. Dengan demikian dari segi kecepatan fungsi *hash* SHA-512 dapat menjadi pilihan yang walaupun bukan merupakan fungsi hash yang paling cepat.

Skema Otentikasi yang Tepat dalam *Intranet.*

dasarkan uraian pada bagian 2 tentang *intranet,* maka dapat diartikan bahwa *intranet* adalah jaringan untuk intern anisasi. Penggunanya adalah komunitas yang saling berkoordinasi dalam sebuah struktur organisasi. Di dalam struktur anisasi tersebut manajemen berwenang menentukan kebijakan yang akan dilaksanakan oleh seluruh komunitas yang komunikasi dalam *intranet.*

anya koordinasi yang baik dan kebijakan manajemen maka memungkinkan antar anggota komunitas yang komunikasi dengan jaringan komputer dapat memiliki password bersama. Pihak manajemen juga dapat merintahkan kepada pihak-pihak tertentu dalam komunitas tersebut untuk menjaga password tersebut.

dasarkan alasan tersebut maka skema otentikasi yang diuraikan di bagian 2 pada Gambar 3 yang dipilih adalah skema yaitu menggunakan password bersama. Selain itu karena pesan M berupa data maka sebelum dilakukan upaya lindungi keotentikan, juga telah dienkripsi dengan algoritma kunci simetri yang merupakan bagian mekanisme njamin privasi. Sehingga pada proses menjamin integrasi dan otentikasi tidak terbebani lagi dengan proses enkripsi g berarti beban komputasinya lebih ringan. Maka skema selain (e) pada uraian 6, tidak cocok untuk dipilih sebab sih memerlukan proses enkripsi. Dengan ringannya beban komputasi di dalam proses otentikasi maka akan dapat ningkatkan kecepatan komunikasi di dalam jaringan komputer.

Kesimpulan.

dak ada suatu mekanisme keamanan yang sempurna. Yang ada hanya mempersulit serangan atau meminimalkan uang terjadinya serangan. SHA-512 merupakan fungsi *hash* yang handal/kuat dan cepat. Kehandalan SHA-512 apai dengan kemampuan menhasilkan nilai *hash* sepanjang 512 bit, yang merupakan nilai *hash* paling panjang yang at dihasilkan oleh fungsi *hash.* Di dalam lingkungan *intranet* SHA-512 dapat digunakan untuk menjamin integritas keotentikan data yang ditansmisikan melalui jaringan komputer dengan penggunaan password bersama antara girim dan penerima pesan. Proses otentikasi dengan SHA-512 yang menggunakan password bersama mempunyai an komputasi paling ringan dibanding skema yang lain karena tidak melibatkan proses enkripsi

Batasan Penelitian

elitian ini dibatasi kajian untuk lingkungan intranet yang didukung oleh kebijakan manajemen untuk menjaga sword bersama dan setiap saat dapat dilakukan perubahan password tersebut oleh manajemen tersebut atau pihak yang eri wewenang oleh pimpinan. Hal itu tidak berlaku pada *ekstranet* yang menghubungkan antar *intranet* organisasi g berbeda, sehingga tidak memungkinkan adanya kebijakan manajamen yang diberlakukan dalam komunitas ggunanya. Untuk lingkungan yang berbeda dengan yang diuraikan di atas maka disarankan tidak menggunakan saword bersama untuk menjamin integritas dan otentikasi pesan. Untuk itu bisa dilakukan kajian lebih lanjut tentang ggunaan sertifikat dijital.

aftar Pustaka

Dai, W. (2009). *Speed Benchmarks for Various Ciphers and Hash Functions.* http://www.weidai.com/, diakses terakhir tanggal 11 Juli 2009.

Losin, P. (1997). *Extranet Design and Implementation*, Sybex Inc.

NIST. (2002). *Secure Hash Standard (SHS).* Federal Information Processing Standards (FIPS) Publication 180-2. U.S. DoC/NIST.

Schneier, B. (2005). *SHA-1 Broken. Schneier on Security.* http://www.schneier.com/blog/archives/2005/02/, diakses terakhir tanggal 12 Juli 2009.

Shcneier, B. (1996). *Applied Cryptography: protocol algorithms, and source code in C*, 2th Edition, John Wiley & Sons, Inc..

Stalling, W. (2006). *Cryptographi and Network Security*, 4th Edition. Prentice Hall, New Jersey.

Wikipedia. (2009). *Cryptographic Hash Function.* http://en.wikipedia.org/wiki/Cryptographic_hash_function. Wikimedia Foundation, Inc. diakses terakhir tanggal Juli 2009.