Kriptanalisis Enkripsi DES dengan Kerberos dalam pengiriman SMS

Ginanjar Fahrul Muttaqin

Teknik Informatika Institut Teknologi Bandung, Ganeca 10,
e-mail: gin2_fm@yahoo.co.id

ABSTRAK

Selama ini kita sering berinterkasi dan berkomunikasi dengan menggunakan SMS. Pada kenyataannya masalah privasi sangat penting dimiliki setiap pengguna layanan ini. Akan tetapi pada kenyataannya ada cara untuk melangkahi privasi seseorang dalam menggukanan layanan SMS. Selain itu banyak cara enkripsi dijalankan untuk mengurangi pengambilan hak-hak sekuritas pengguna layanan SMS. Dalam hal ini beberapa metode dikembangkan, yaitu dengan penerapan DES untuk mengenkripsi paket-paket data yang akan dikirim. Atau dengan menggunakan kerberos untuk mengenkripsi interkoneksi antar jaringan sebelum mentransmisikan data. Beberapa cara tersebut ternyata masih bisa dipecahkan dan selalu ada celah untuk menghancurkan sistem pengamanan pengiriman paket SMS. Makalah ini dibuat untuk membahas bagaimana beberapa cara yang mungkin dilakukan untuk melangkahi privasi seseorang dalam menggunakan layanan SMS. Selain itu makalah ini juga membahas bagaimana masalah-masalah itu kemudian secara simultan diselesaikan dengan mempertinggi tingkat keamanan pengiriman paket SMS.

Kata kunci: DES, Kerberos, SMS,

1. PENDAHULUAN

Tukar menukar informasi lewat jaringan sudah sangat diutamakan sekarang. Selain reliability yang ditingkatkan, kecepatan dan keleluasaan transfer data semakin tinggi seiring berkembangnya teknologi.

Salah satu media pengiriman data adalah dengan mengirimkan pesan melalui layanan SMS. Menurut statistik, sampai tahun 2008, ada 4.1 juta triliyun teks SMS yang dikirimkan. SMS has become a massive commercial industry dan lebih dari 81 triliyun dollars biaya yang dikeluarkan sampai tahun 2006, dengan harga rata-rata per pengiriman sms adalah 0,11 USD. Bahkan sampai teknologi pengiriman pesan seperti *messenger*, email dan sejenisnya berkembang, teknologi SMS masih tetap bertahan sampai tahun 2010. Hal ini menunjukkan betapa penting dan dipertahankannya teknologi ini sampai sekarang.

Masalah umum yang selalu menjadi isu dalam pengiriman data adalah masalah sekuritas. Setiap data yang terkirim dari satu perangkat ke perangkat lain ternyata melewati jalur pengiriman data yang berpotensi pencurian data digital. Penulis akan menerangkan beberapa peluang pencurian data dalam pengiriman paket SMS.

Salah satu metode untuk mengurangi potensi pencurian data SMS yang terkirim di jaringan adalah dengan melakukan enkripsi data. Penulis akan membahas salah satu cara enkripsi data dengan menggunakan DES. DES itu sendiri termasuk algoritma enkripsi block cipher.

Dalam makalah ini penulis akan menerangkat tentang DES dan penerapanannya dalam keamanan jarinnga SMS. Selain itu penulis juga akan membahas bagaimana penerapan kerberos pada transaksi data di jaringan.

2. PRINSIP DASAR

2.1 *Data Encryption Standard*

Sejarah DES

Pada tahun 1972 isu pencurian data digital sangat marak di Amerika. Beberapa masalah tentang pencurian data, privasi dan modifikasi berkembang tidak terkontrol. Sampai pada akhirnya pada saat itu diadakan sayembara untuk mencari teknik enkripsi data yang sulit untuk dipecahkan.

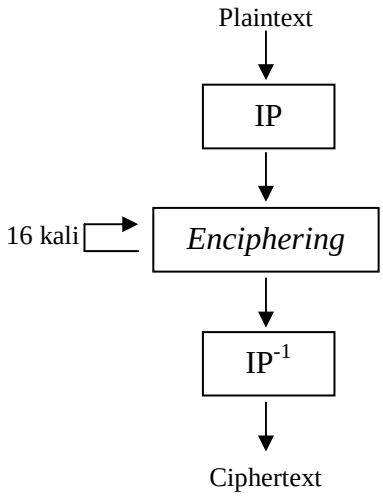
IBM mengembangkan *Data Encryption Standard* yang merupakan pengembangan algoritma *Lucifer*. Pada saat itu *Data Encryption Algorithm* akhirnya disahkan sebagai algoritma standar yang sulit dipecahkan saat itu oleh NSA USA.

Mekanisme kerja DES

Data Encryption Standard menggunakan *Data Encryption Algorithm*. Algoritma ini termasuk metode *block cipher algorithm*. Pada dasarnya block ciperh akan mengoperasikan data dalam skala *binnary* dan

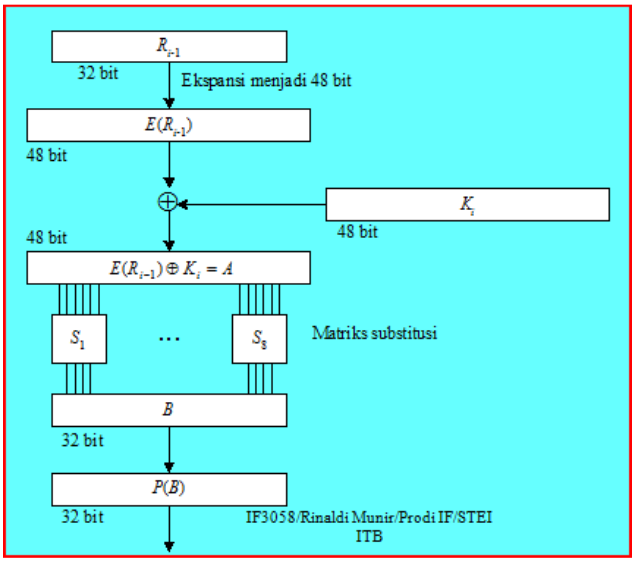
mengelompokkannya ke dalam blok-blok dengan jumlah tertentu.

DES menggunakan panjang blok 64 bit dengan panjang kunci 56 bit dari 64 bit kunci eksternal. Secara umum skema global algoritma terlihat pada gambar di bawah ini:



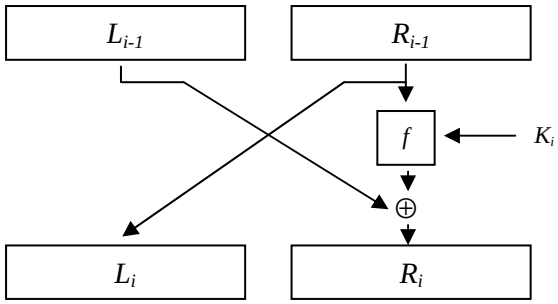
Gambar 1. Skema DES

Proses *Enciphering* yang terjadi akan mengubah blok-block menjadi terenkripsi dengan beberapa tahap seperti berikut ini, anggap sebagai komputasi fungsi f:



Gambar 2. Fungsi Enkripsi pada Skema DES

Fungsi f akan mengacak isi dari setiap blok. Untuk memudahkan dekripsi, fungsi f ini dimasukan kedalam jaringan feistel.



Gambar 3. Jaringan Feistel pada Skema DES

Proses enkripsi akan menghasilkan ciphertext dengan panjang blok yang sama.

Keamanan DES

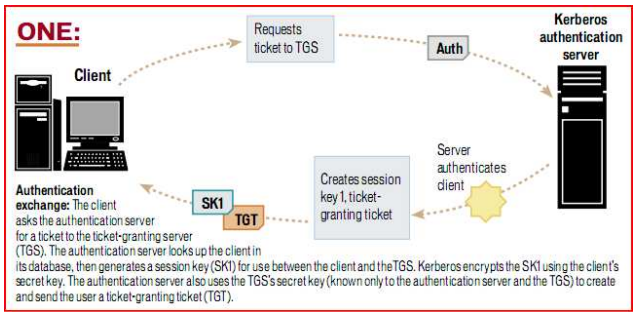
Kelemahan DES dan algoritma block cipher lainnya adalah dari panjang kunci yang dilakukan untuk enkripsi. DES menggunakan kunci dengan panjang 56 bit. Sehingga untuk memecahkannya dengan menggunakan *brute force* kunci dapat ditemukan dengan 2^{56} pencarian.

Untuk perkembangan sekarang DES sudah tidak bisa dinyatakan aman. Hal ini disebabkan karena sistem komputasi sudah sangat tinggi sehingga kunci dapat dicari dan dipecahkan.

2.2 Kerberos dalam jaringan

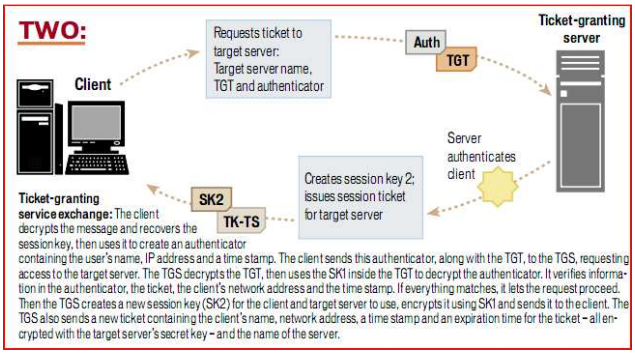
Kerberos adalah sebuah protokol *network authentication.* Kerberos dikembangkan di MIT dan sudah menjadi produk yang dirilis untuk dipergunakan dalam keamanan jaringan. Sebelum dikembangkannya kerberos jaringan mengalami kendala dari segi transfer data. Kerberos mengembangkan sistem autentikasi untuk mengidentifikasi dan mengamankan transaksi antara client dan server dengan menggunakan algoritma yang dirahasiakan.

Mekanisme kerja kerberos



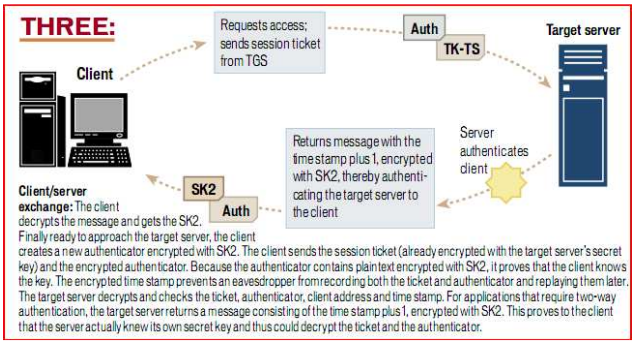
Gambar 4. Request Ticket Kerberos

Pada tahap pertama *client* meminta *request* TGS ke *server* untuk meminta *authenteication*. Setelah itu dibuat *session key 1* untuk mendapatkan *ticket.*



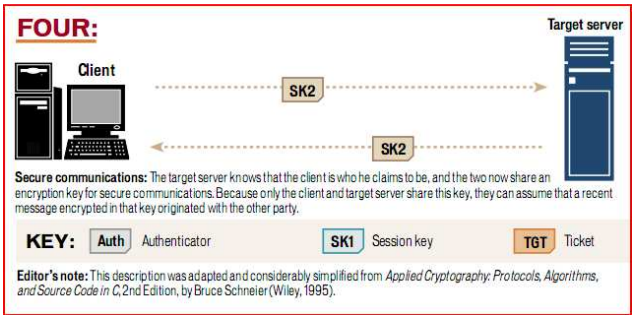
Gambar 5. Autentikasi 1 untuk Session Key 1

Pada tahap ini dibuat *session key 2* untuk menentukan *target server.*



Gambar 5. Autentikasi II untuk Session Key 2

Pada tahap ini *server* yang akan mengautentikasi *client* dengan mendapatkan *ticket* dari *client.*



Gambar 6. Transaksi Terenkripsi dengan Kerberos

Untuk seterusnya *session* transaksi antara *server client* dengan menggunakan *session key 2.*

Kerberos telah bisa digunakan dalam sistem operasi BSD, windows, dan beberapa vendor lainnya. Kerberos juga bsia dikembangkan dalam penerapan transmisi data SMS.

2.3 Mekanisme pengiriman SMS dengan jaringan

Short Message Service adalah sebuah layanan untuk berkomunisasi dengan perangkat *mobile.* Membicarakan SMS berarti membicarakan GSM karena pada dasarnya SMS menggunakan GSM untuk mengirimkan paket data.

Dalam pengiriman paket data SMS menggunakan sistem *store and forward system.* Setiap pengiriman data selalu melibatkan *carrier. Carrier* adalah satu *provider* yang menyediakan layanan SMS.

Store and forward message delivery

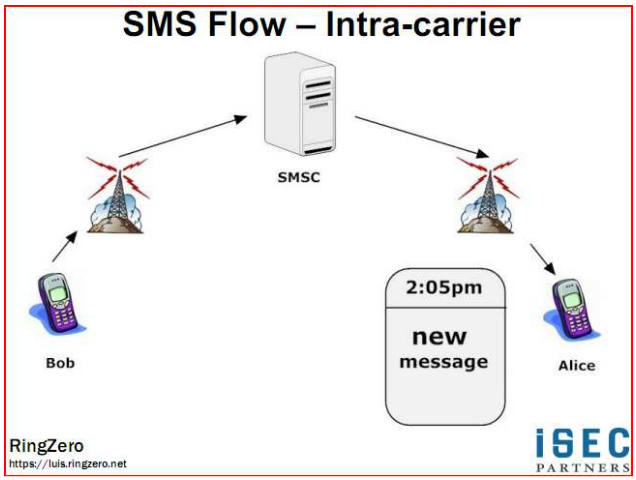
Carrier yang dimaksud terdiri dari SMSC (*Short Message Service Center*) sebagai *sender submit.* SMSC bertindak sebagai pengirim dan penerima antar SMSC dan antara SMSC dengan *recipient* dalam hal ini pengguna perangkat.

Ada dua forma yang ada pada SMSC yaitu:

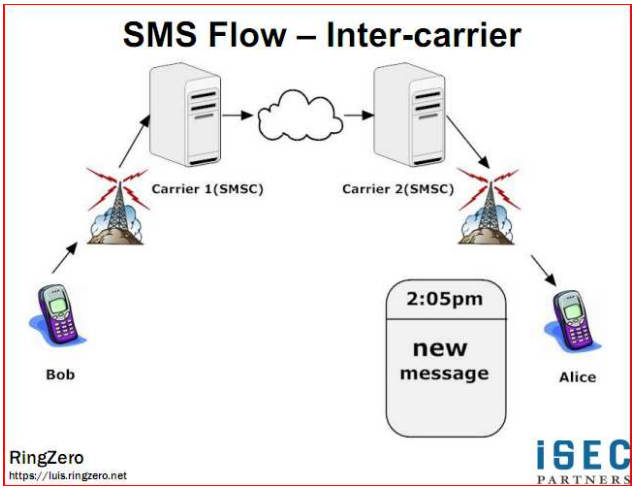
- SMS_SUBMIT untuk mengirimkan paket data SMS dari *phone* ke SMSC
- SMS_DELIVER untuk mengirimkan paket data SMS dari SMSC ke *phone*

GSM dalam pengiriman SMS memiliki dua buah processor, yaitu untuk GUI, dan menangani modem untuk mentransmisikan data.

Berikut ini skema pengiriman data SMS dari satu perangkat ke perangkat lain.

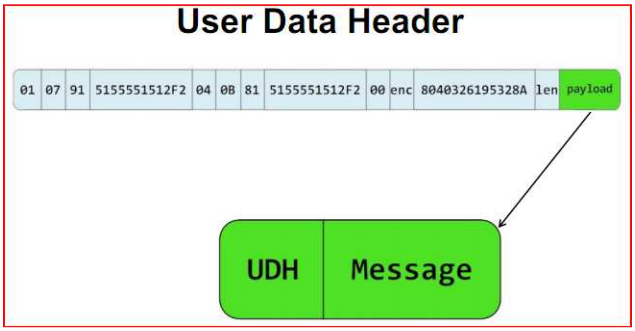


Gambar 7. Skema SMS dalam Satu Carrier

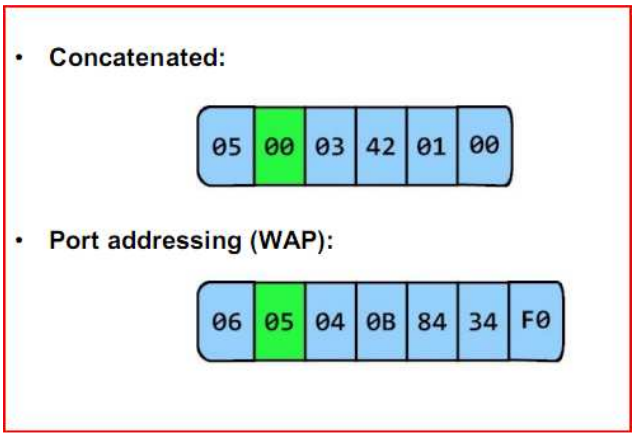


Gambar 8. Skema SMS dalam Carrier Berbeda

Paket yang dikirimkan memiliki format yang baku. Format ini akan memudahkan perangkat membaca dan mendeskripsikan isi dari pesan yang dikirim. Berikut format header dari sebuah paket data SMS yang dikirimkan:



Gambar 8. User Data Header SMS



Gambar 9. WAP Port Addressing bagian dari UDH

3. ANALISIS

3.1 Bagaimana pesan yang terkirim lewat SMS diserang

Prinsip keamanan informasi menyangkut beberapa hal penting yaitu, sekuritas, privacy, dan integritas. Sekuritas terkait siapa yang memiliki hak untuk mengakses sebuah data. Privacy meyangkut siapa yang berhak memodifikasi data. Sedangkan integritas terkait dengan keutuhan data sehingga data tetap asli dan sesuai dengan kebutuhannya.

Ada tiga jenis serangan yang bisa diperoleh dalam pengiriman paket data SMS melalui jaringan:

1. Mempengaruhi kecepatan pengiriman paket pada *carrier*, sehingga pesan terkirim dengan lambat
2. Pengaturan *cost* atau tarif, dengan mempermurah tarif individu. Atau bisa juga melakukan *fuzzing thousands of messages* sehingga tarif menjadi sangat mahal.
3. Menambahkan, mengurangi, dan memodifikasi paket data sehingga sekuritas bisa dijebol. Misalkan dengan membuka log pada pengiriman paket atau *sniffing trafic.*

Dari ketiga jenis serangan tersebut yang akan lebih dibahas adalah mengenai *sniffing trafic*. Data yang dienkripsi dengan DES akan menyebabkan UDH (*User Data Header*) sudah tidak bisa diterjemahkan kembali jika diambil di tengah transaksi data.

3.2 Beberapa cara yang bisa digunakan untuk mencuri data SMS

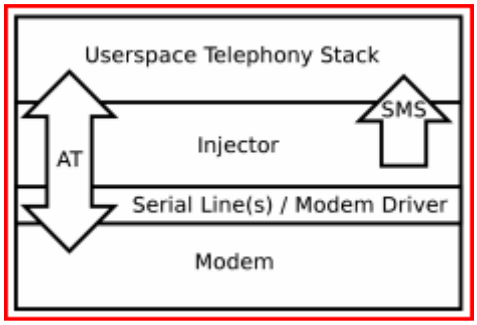
Gambar 10. Alat Sniffing SMS

Ada beberapa cara yang bisa digunakan untuk menyerang pengiriman data dan mendapatkan data yang terkirim dari *client* ke *server.*

SMS Injection

Cara ini akan menempatkan seseorang di tengah-tengah telephone sehingga terjadi penyisipan SMS melalui +CMT result code.

Berikut contoh skema SMS injector via WiFi:



Gambar 11. SMS Injector via WiFi

iPhone Injector

Injector daemon digunakan untuk membuka koneksi modem melalui "/dev/dlci.[h5|spi]-baseband.3,4" atau dengan menggunakan domain socket dari CommCenter UNIX.

Android Injector

Menggunakan daemon melalui MITM dengan mengganti "/dev/smd0" menjadi "/dev/smd0real", membuka "/dev/smd0real" dan membuat *fake* "/dev/smd0". Merestart kembali "/system/bin/rild" dan membuka kembali "/dev/smd0".

Windows Mobile Injector

Windows Mobile lebih mudah untuk diinjeksi yaitu dengan cara mengubah *serial device driver*. Pengubahan ini menggunakan perintah *open source* untuk *logging driver*. Kemudian membuat kembali serial driver untuk menerima pesan dari modem.

Langkah selanjutnya adalah mengubah isi dari log-driver dengan SMS Injection. Penambahan ini dengan menggunakan *SMS message submission via TCP socket.*

SMS Fuzzing

SMS *fuzzing* akan menyebabkan seorang *client* mendapatkan pesan SMS secara terus menerus, SMS yang berhalaman besar, atau mendapatkan *voice mail notification* secara terus menerus dalam satu waktu.

Port yang digunakan adalah TCP/IP 0-65535, dengan cara mengirimkan "sampah" ke port secara random. Misalkan dengan WAPpush di 2948. Lalu melakukan Port Scanning.

3.3 Kriptanalisis DES dengan menggunakan Kerberos

Biham dan Shamir pada tahun 1991 mencoba memecahkan DES dengan menggunakan berbagai plaintext yang dipilih. Cipher Block DES kemudian digunakan untuk mengenkripsi berbagai plaintext tersebut dalam sebuah jaringan Kerberos.

Pada beberapa keadaan bahkan dengan algoritma berantai kriptanalisis yang digunakan Biham dan Shamir hampir efektif. Alasannya karena data yang terenkripsi pada blok langsung didahului dengan blok pertama pada data field yang terautorisasi sebelum *Kerberos ticket* didapat.

Hal ini hampir tidak mungkin, untuk itu kita diskusikan bagaimana caranya setiap data block yang akan dianalisis didapatkan sebelum *ticket* didapatkan. Sebenarnya setiap kali kita enkripsi setiap versi dari blok seperti halnya DES, kemudian kita pilih sebuah plaintext pada seluruh data field yang terautorisasi. Sehingga ketika data tersebut di-XOR-kan dengan data terenkripsi sebelumnya hasilnya adalah plaintext yang harusnya dienkripsi.

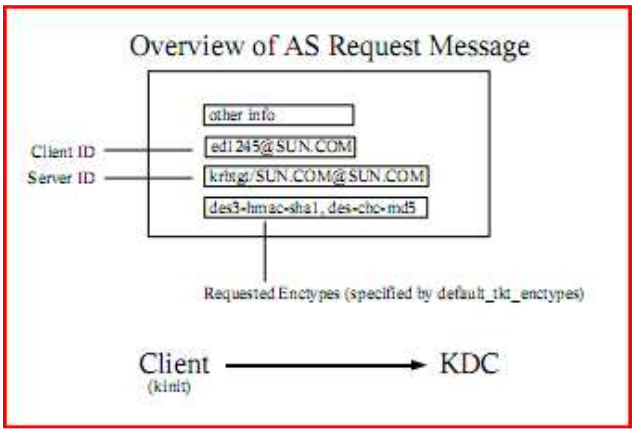
Hal ini bisa tercapai jika tidak ada *confounder*, *checksum*, dan jika kunci yang berada di *session key 1* telah direlokasi setelah mengautorisasi data field. Pada kasus ini jika kita membuat *ticket request*, tidak ada data yang bisa didahului sebelum autorisasi data field yang bisa diubah, dan akan hanya mendapatkan satu *ticket* dalam nilai konstan blok yang terenkripsi.

Misalkan ukuran dari kunci sangan kecil, sehingga pada *birhtday paradox* tidak akan memakan waktu yang lama untuk membuat fungsi "*random*". Pilih kembali kunci yang sama kemudian jika kunci diautorisasi sebelum data field, kita akan bisa mengenkripsi pesan text beberapa waktu sampai nilai blok tersebut berhasil dienkripsi dan membuat sebuah kunci. Pada saat itulah kita bisa memperlihatkan ciphertext yang terautorisasi dari data field. Hal yang sama tidak bisa diulang untuk confounder muncul kembali dan mengaplikasikan metode ini.

3.5 Teknik penggunaan DES memanfaatkan kerberos dengan Java framework

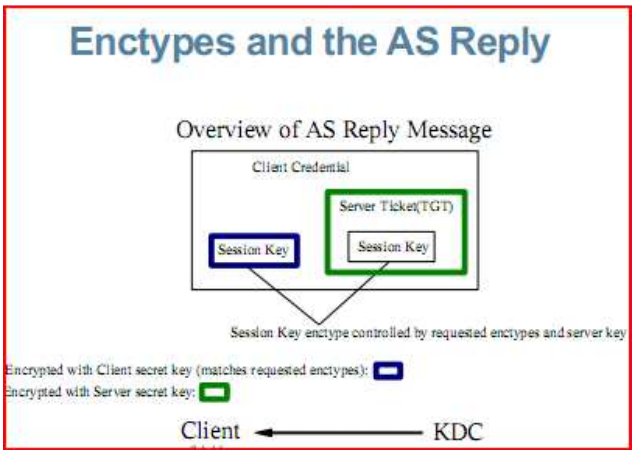
Data terenkripsi sebagai *AS request*

Berikut ini salah satu contoh AS *request message* yang digunakan pada Kerberos:



Gambar 12. Representasi AS Request pada Java

Selain itu berikut adalah bagaimana *AS reply* didefinisikan:



Gambar 13. AS Request Terenkripsi pada Java

Mekanisme ini bisa dipelajari lebih lanjut untuk menggunakan kerberos dengan Java Framework.

IV. KESIMPULAN

Kriptografi adalah ilmu untku mempelajari bagaimana mengenkripsi sebuah data menjadi data yang tidak dimengerti. Ilmu kriptografi seringkali digunakan untuk menjaga privasi seseorang atas data yang dia miliki.

Media komunikasi paling besar yang digunakan oleh manusia sejak abad 20-an adalah dengan menggunakan SMS. Layanan SMS pada umumnya adalah mekanisme pengiriman paket-paket data dari sebuah *client* kepad *client* lain melalui SMSC pada SMS Gateway dengan perantara sebuah provider.

Pengiriman data dari satu *Carrier* ke *Carrier* lain berpotensi untuk diserang olah pihak luar. Begitu halnya dengan pengiriman paket data SMS. Hal ini sangat berpotensi terjadi. Beberapa algoritma kriptografi digunakan untuk mengenkripsi data yang terkirimkan, salah satunya adalah dengan DES.

Pengiriman data hanya dengan enkripsi data tidak cukup untuk mencegah penyalahgunaan data, oleh karena itu dibuat kembali mekanisme pengamanan jaringan pada mode transaksi, yaitu dengan menggunakan Kerberos. Kerberos akan mengenkripsi setiap hubungan antara *server-client* pada setiap koneksi dengan menggunakan dua buah *session key.*

Secanggih apapun sebuah mekanisme pengamanan informasi selalu ada cara bagaimana memecahkannya. Dari waktu ke waktu kedua hal itu saling kejar mengejar. Oleh karena itu, penulis berharap dengan menambah pengetahuan melalui makalah ini diharapkan pembaca dapat menyadarinya dan selalu mengikuti perkembangan teknologi. Bagi teknologi pengamanan informasi, mereka yang terdepanlah yang menguasai panggung permainan.

Dengan segala kekurangannya penulis memohon maaf dan semoga makalah ini bermanfaat untuk pembaca. Terimakasih.

REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] Kay, Jennifer, *Cryptanalysis Techniques: An Example Using Kerberos*, Carnegie Mellon University, Pittsburgh, 1995

[3] Barkan, Elad, *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication**, Israel Institut of Technology

[4] Azim, Akramul dkk, *Exploiting Vulnerabilities and Security Mechanisms in Internet based SMS capable Cellular network*, IJCSNS, 2007

[5] Mulliner, Collin, *Injecting SMS Messages into Smart Phones for Security Analysis*, USENIX WOOT, 2009

[6] Lackey, Zane, *Attacking SMS*, BlackHat USA, 2009

[7] http://web.mit.edu/Kerberos/