EKSPLORASI DAN ANALISIS KEAMANAN BLACKBERRY MESSENGER UNTUK PENGGUNAANNYA DI INDONESIA SAAT INI.

Jonathan Ery Pradana / 13508007
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18007@students.if.itb.ac.id

Penggunaan Smartphone Blackberry di Indonesia sekarang sudah sangat besar, perkembangannya pun melambung jauh dikarenakan beberapa fitur khusus yang disediakan oleh Research In Motion (Developer Blackberry). Diantara fitur itu, terdapat satu fitur yang menjadi andalan Blackberry terutama dalam pasarannya di Indonesia, fitur tersebut adalah Blackberry Messenger atau biasa disebut BBM. BBM adalah sebuah aplikasi instant messaging yang ditawarkan secara eksklusif khusus untuk pengguna handset Blackberry. Untuk setiap handsetnya, Blackberry memiliki sebuah PIN yang akan menjadi ID untuk aplikasi BBM. Di Indonesia, BBM sudah menjadi hal yang publik digunakan dimana-mana, baik oleh kalangan kerja, maupun pelajar. Akan tetapi, pada awal bulan 2011, muncul sebuah isu publik yang mengatakan bahwa BBM memiliki fitur enkripsi yang akan memudahkan pelaku kejahatan dan terorisme di Indonesia beroperasi. Dengan melakukan analisis terhadap fitur Blackberry ini, dan enkripsi apa yang digunakan didalamnya, akan disimpulkan apakah Blackberry ini aman digunakan di Indonesia saat ini.

Index: Blackberry, Indonesia, Pelaku Kejahatan, Enkripsi

I. PENDAHULUAN

Blackberry merupakan suatu media komunikasi yang paling marak di Indonesia saat ini. Secara umum, pengguna Blackberry di Indonesia sudah cukup banyak, sebagian besar hal ini disebabkan oleh adanya fitur Blackberry Messenger atau biasa disingkat BBM yang diberikan oleh Blackberry. Akhir-akhir ini, dari sekian banyak pengguna Blackberry di Indonesia, pemerintah menyoroti penggunaan Blackberry di Indonesia untuk media komunikasi terorisme. Hal ini kemudian menimbulkan banyak sekali isu yang beredar di kalangan masyarakat, salah satunya adalah terkait adanya isu yang menyatakan bahwa Blackberry akan ditarik peredarannya dari Indonesia. Masalah ini menimbulkan banyak persepsi negatif di kalangan masyarakat dan memunculkan ketakutan akan pencabutan handset Blackberry bagi orang-orang yang masih sangat membutuhkan fitur Blackberry Messenger ini untuk kehidupan sehari-harinya.

Pada makalah ini penulis akan melakukan analisis terhadap fitur Blackberry Messenger ini terkait sistem keamanannya terutama fitur enkripsi yang ada didalamnya. Analisis dari saya ini nantinya akan menghasilkan suatu kesimpulan apakah Blackberry Messenger 'aman' atau 'tidak aman' untuk digunakan di Indonesia pada saat ini terkait dengan fitur enkripsi yang disediakan oleh Blackberry sendiri untuk aplikasi Blackberry Messenger, sekaligus saran-saran yang dapat mendukung keamanan pesan ini, sehingga pesan dapat terjaga dan terkontrol.

II. PERUMUSAN MASALAH

Berikut akan dipaparkan beberapa kutipan artikel di Indonesia dalam kurun waktu saat Blackberry akan diancam untuk dicabut peredarannya dari Indonesia akibat fitur enkripsinya.

1. Artikel 1: [1]

Data Encryption Is Reason For BlackBerry And Skype Ban In India?

It looks like the ability to encrypt data in BlackBerries and Skype--the same science behind the protection found in drive encryption software like AlertBoot--is grounds for banishment from the Indian subcontinent...if the companies do not play nice.

Give Us a Backdoor or Else...

Supposedly, India's Department of Telecommunications will ask Skype and Research in Motion (RIM, the company behind the BlackBerry) for access so that India's security and intelligence agencies may tap the data.

If the companies do not comply in 15 days, they could "face a ban in India." The DOT denied the story via a spokesperson.

This is not the first time the makers of the BlackBerry have been at loggerheads with the Indian government. A similar situation developed back in 2008. RIM noted at that time that they had no control over decrypting data--the encryption key was created and used by the user of the device, and RIM had put itself outside the loop.

Similarly, Skype uses encryption to protect all calls via their Skype network. If I recollect correctly, the German government has been having a heck of a time trying to eavesdrop on Skype calls. I seem to recall that they announced that they were successful in tapping those calls, but it sounded as if they had to use a specially-designed Trojan, essentially exploiting the fact that Skype's encrypted calls must decrypt at some point for people to hear each other.

Encryption is a Powerful Security Tool

As you can see, encryption is a powerful tool for ensuring the protection and confidentiality of data. It's the reason why so many governments use the same technology to protect their own information and seek to find a way around it when someone else uses it.

If you or your company needs to protect data, you could do a whole lot worse when it comes to data security: protecting SSNs, financial account numbers, medical data, etc. can be enhanced with the right encryption software.

2. Artikel 2: [2]

Menurut Tifatul, beberapa poin penting yang harus dipatuhi pihak Research in Motion (RIM) salah satunya adalah harus menghormati dan mematuhi peraturan perundangan-undangan yang berlaku di Indonesia. "Yakni terkait dengan UU No 36/1999, UU No 11/2008, dan UU No 4/2008," tulisnya untuk poin pertama.

Selain itu, mantan Presiden PKS ini juga meminta agar RIM membuka perwakilan di Indonesia. Ia beralasan, pelanggan RIM di Indonesia untuk BlackBerry mencapai 2 juta lebih.

Poin berikutnya, Tifatul juga meminta agar RIM membuka pusat layanan (service centre) di Indonesia. Keinginan itu agar memudahkan melayani pelanggan yang berada di Indonesia.

Permintaan berikutnya, Tifatul juga meminta agar RIM merekrut dan menyerap tenaga kerja Indonesia secara layak dan profesional. "Kita minta RIM agar sebanyak mungkin menggunakan konten lokal Indonesia, khususnya mengenai software," cetusnya.

Permintaan lainnya, Tifatul juga meminta agar RIM membangun server (repeater) di Indonesia, agar aparat hukum dapat melakukan penyelidikan terhadap pelaku kejahatan termasuk koruptor.

Sejatinya, bukan kali ini saja Kementerian Kominfo menimbulkan polemik terkait RIM. Sebelumnya tentang rencana penyadapan BlackBerry Messenger(BBM). Sama dengan ide yang saat ini muncul, kala itu juga terjadi penolakan keras dari publik.

Sumber *INILAH.COM* di Kemenkominfo, sejatinya, isu utama dari pemblokiran BB terletak pada upaya penegakan hukum. Karena rencana penyadapan percakapan BBM sejatinya atas permintaan dari Komisi Pemberantasan Korupsi (KPK). "Ada kasus, KPK akan menyelidiki salah satu target, namun gagal karena komunikasi yang bersangkutan beralih dari telepon seluler ke BBM," katanya.

Langkah Tifatul yang *misleading* ini sejatinya bukan berdiri sendiri. Jika memang KPK berkepentingan dalam penegakan hukum, bisa saja, KPK dan Kementerian Kominfo menjelaskan secara bersama-sama ke publik terkait agenda yang jauh lebih penting daripada pemblokiran situs porno, yakni penegakan hukum. [mdr]

3. Artikel 3: [3]

NASIONAL

Senin, 10 Januari 2011 , 06:16:00

Blokir Blackberry Sudah Harga Mati

JAKARTA - Rencana pemerintah memblokir izin operasi produsen Blackberry, Research In Motion (RIM) di Indonesia per 17 Januari sudah harga mati. Menteri Komunikasi dan Informatika (Menkominfo) Tifatul Sembiring mengatakan sudah tidak ada toleransi lagi kepada pabrikan telepon seluler asal Kanada itu. Tifatul mengimbau publik bersiap jika pada pekan depan fasilitas Blackberry yang disediakan sejumlah operator tidak bisa dioperasikan lagi di Indonesia.

"Karena sejauh ini terkesan RIM mengulur-ulur waktu untuk menjalankan komitmen mereka. Pemerintah tidak akan mundur selangkah pun," kata Tifatul di Jakarta Minggu, Minggu (9/1).

Seperti diwartakan, Kemenkominfo akan mencabut izin usaha RIM dalam dua pekan mendatang karena mereka menolak memblokir akses terhadap situs porno. Dalam pertemuan terakhir, RIM mengeluhkan besarnya biaya dan investasi untuk memblokir konten pornografi secara khusus di wilayah Indonesia.

Secara umum, Tifatul memiliki tujuh permintaan kepada RIM. Antara lain, agar RIM menghormati Peraturan UU 36/1999, UU 11/2008 dan UU 44/2008, RIM juga harus membuka kantor di Indonesia, RIM harus membuka service center, RIM juga wajib merekrut tenaga kerja lokal. Selanjutnya, Tifatul meminta RIM menggunakan konten lokal Indonesia, khususnya software, Rim juga wajib memasang software blocking situs porno.

"Dan yang terpenting, RIM agar membangun server/repeater di Indonesia, sehingga aparat penegak hukum bisa melakukan penyelidikan kepada pelaku kejahatan," tegas dia.

4. Artikel 4: [4]

INILAH.COM, Jakarta - Pengamat menilai kasus dengan Research In Motion tak sebatas blokir pornografi dan server. Pemerintah menginginkan kunci enkripsi untuk mengakses data pengguna.

TERKAIT

- Inilah Sisi Negatif Memiliki Smartphone
- Bocor, Samsung Galaxy S2 Mini Rilis April
- Yusuf Supendi Ungkap Poligami 'O'
- Solusi RIM Pada Browser Rentan Bajak BlackBerry
- Gawat! Browser BlackBerry 6 Rentan Dibajak Peretas

Menurut Direktur Eksekutif Eddy Thoyib, saat dihubungi *INILAH.COM*, kemungkinan besar pemerintah tidak hanya memblokir pornografi. Namun juga kode enkripsi, jika permintaan server lokal dipenuhi oleh produsen BlackBerry, Research In Motion (RIM).

"Jika server dipenuhi, kita juga menginginkan kode enkripsi. Bagaimana kita membuka data kalau nggak memperoleh kuncinya. Ini cara melindungi masyarakat. Tidak cuma soal pornografi," kata Eddy.

Muncul indikasi pemerintah menginginkan akses ke data BlackBerry untuk mencari tahu jalur komunikasi pelaku kejahatan, teroris dan koruptor, misalnya. BlackBerry dinilai 'sangat aman' karena semua data tersimpan di ***server*** milik BlackBerry di Kanada.

Hal senada juga diungkapkan anggota Badan Regulasi Telekomunikasi Indonesia (BRTI) Heru Sutadi.

"Server diinginkan di Indonesia untuk mendapatkan tarif yang lebih murah serta keamanan bagi pengguna BlackBerry. Jika ada kejahatan dan teroris, data komunikasi via BlackBerry bisa diketahui. Sekarang tidak bisa karena *server* ada di Kanada," ujar Heru Sutadi.

Pengguna BlackBerry di Indonesia saat ini mencapai dua juta orang atau 7% dari 21 juta pengguna global di seluruh dunia. Mitra RIM di Tanah Air antara lain Telkomsel, Indosat, XL Axiata, Natrindo Telepon Seluler (Axis), Hutchison CP Telecom (Three) dan Smart Telecom.

BRTI meminta RIM melakukan empat hal yakni pengurusan izin telekomunikasi termasuk penyediaan jasa internet (ISP / Internet Service Providers), pembatasan konten negatif, pembangunan server di Indonesia serta menentang penyebaran kejahatan seperti terorisme dan korupsi di BlackBerry. [vin]

5. Artikel 5 : [5]

RIM: your BlackBerry data is secure, even from governments

By: Andrew Munchbach | Aug 2nd, 2010 at 05:30PM **View Comments**

Filed Under: BlackBerry, Mobile, RIM, Security

The Wall Street Journal is reporting that BlackBerry maker Research In Motion has issued a statement to its customers letting them know just how secure their data is. The handset maker reminded everyone that "no one, including RIM" could access BlackBerry user data as it is encrypted without a master key, and that it would "be unable to accommodate any request" for access to the data. RIM continued, the system is designed "to exclude the capability for RIM or any third party to read encrypted information under any circumstances." The statement comes on the heels of this weekend's decision by the United Arab Emirates to suspend BlackBerry data services in the country due to reasons related to national security. RIM has not released an official statement regarding talks with the UAE citing the confidentiality of discussions at the government level.

Berdasarkan beberapa artikel tersebut, dinyatakan bahwa fitur Blackberry Messenger ini dianggap kurang aman oleh beberapa entitas pemerintahan, baik di Indonesia, maupun diluar Indonesia (seperti India). Bahkan di Artikel 5 [5], terdapat statement bahwa "Your Blackberry data is secure, even from governor". Dalam hal ini, penulis akan mencoba menganalisis lebih jauh fitur yang ditawarkan oleh Blackberry ini terutama di sisi keamanan pengiriman pesannya dengan mengacu pada beberapa fakta yang sudah dipaparkan di beberapa kutipan artikel diatas.

III. DASAR TEORI

III.I Blackberry [6],[7]

BlackBerry adalah perangkat selular yang memiliki kemampuan layanan push e-mail, telepon, sms, Menjelajah Internet, dan berbagai kemampuan nirkabel lainnya. Penggunaan gadget canggih ini begitu fenomenal belakangan ini, sampai menjadi suatu kebutuhan untuk fashion. BlackBerry pertama kali diperkenalkan pada tahun 1997 oleh perusahaan Kanada, Research In Motion (RIM). Kemampuannya menyampaikan informasi melalui jaringan data nirkabel dari layanan perusahaan telepon genggam hingga mengejutkan dunia.

Sejarah

BlackBerry pertama kali diperkenalkan di Indonesia pada pertengahan Desember 2004 oleh operator Indosat dan perusahaan Starhub. Perusahaan Starhub merupakan pengejewantahan dari RIM yang merupakan rekan utama BlackBerry. Pasar BlackBerry kemudian diramaikan oleh dua operator besar lainnya di tanah air yakni Excelcom dan Telkomsel. Akibat tuntutan pemerintah Indonesia, Blackberry akhirnya membuka kantor perwakilan di Indonesia pada November 2010.

Keunggulan

Produk yang menjadi andalan utama dan membuat BlackBerry digemari di pasar adalah surat-e gegas (push e-mail). Produk ini mendapat sebutan surat-e gegas karena seluruh surat-e baru, daftar kontak, dan informasi jadwal (calendar) "didorong" masuk ke dalam BlackBerry secara otomatis.

Seperti yang telah disebutkan di atas mengenai keunggulan dari BlackBerry, yaitu push e-mail. Dengan push e-mail semua e-mail masuk dapat diteruskan langsung ke ponsel. E-mail juga sudah mengalami proses kompresi dan scan di server BlackBerry sehingga aman dari virus. Lampiran file berupa dokumen Microsoft Office dan PDF dapat dibuka dengan mudah. Sebuah e-mail berukuran 1 MB, jika diterima melalui push e-mail dapat menjadi 10 kb dengan isi yang tetap.

Pengguna tidak perlu mengakses Internet terlebih dulu dan membuka satu persatu surat-e yang masuk, atau pemeriksaan surat-e baru. Hal ini dimungkinkan karena pengguna akan terhubung secara terus-menerus dengan dunia maya melalui jaringan telepon seluler yang tersedia. Alat penyimpanan juga memungkinkan para pengguna untuk mengakses data yang sampai ketika berada di luar layanan jangkauan nirkabel. Begitu pengguna terhubung lagi, BlackBerry Enterprise Server akan menyampaikan data terbaru yang masuk.

Kelebihan lainnya adalah kemampuan BlackBerry yang dapat menampung e-mail hingga puluhan ribu tanpa ada risiko hang, asalkan masih ada memori tersisa. BlackBerry juga bisa digunakan untuk chatting. Mirip dengan Yahoo Messenger, namun dilakukan melalui jaringan BlackBerry dengan memasukan nomor identitas.

Semua layanan BlackBerry ini dikenal sangat aman baik e-mail, chatting, maupun browsing. Untuk browsing Internet, data-data dari website sudah dikompresi sehingga lebih cepat dibuka.

Gambar 1: Blackberry Onyx

Fasilitas lain yang menjadi andalan BlackBerry adalah pesan instan. Yahoo Messenger, Google Talk dan Skype kini telah menjadi rekanan dengan BlackBerry. Teknologi terkini memang memungkinkan kita untuk "mengobrol" (chatting) di Internet melalui telepon genggam dan Personal Digital Assistant (PDA). Tetapi yang berbeda pada BlackBerry adalah proses instalasi lengkap yang bisa dilakukan nya melalui jaringan nirkabel.

Melihat fenomena BlackBerry yang digemari masyarakat karena keunggulan fasilitas komunikasinya, membuat banyak perusahaan IT berkembang dan berlomba-lomba menciptakan aplikasi yang paling mutakhir untuk pengguna BlackBerry. Salah satu diantaranya adalah aplikasi Intar. Keunggulan lain juga hadir melalui teknologi kompresi yang menyebabkan biaya akses menjadi murah dan pemberitahuan jawaban pesan melalui tanda getar pada BlackBerry.

Penggunaan BlackBerry semakin meluas dengan hadirnya fasilitas koneksi BlackBerry (BlackBerry Connect). Dengan BlackBerry Connect, pengguna tidak lagi harus menggunakan perangkat genggam BlackBerry untuk memanfaatkan BlackBerry Internet Solution. Pengguna hanya perlu menginstalasi BlackBerry Connect pada smartphone merek apapun yang dimiliki, kita bisa memanfaatkan BlackBerry Internet Solution.

Terdapat perbedaan dengan handset BlackBerry, di mana untuk handset non BlackBerry apabila aplikasinya membutuhkan koneksi GPRS/EDGE/3G maka koneksi akan dikenakan biaya GPRS sesuai operator. Jumlah email yang bisa diintegrasikan jika menggunakan HP BlackBerry adalah 10 email

account dan jika menggunakan BlackBerry Connect tergantung memori HP.

BlackBerry Enterprise Server (BES)

Perangkat genggam BlackBerry terintegrasi pada sistem e-mail yang terorganisasi melalui paket perangkat lunak yang disebut BlackBerry Enterprise System (BES). BES dapat digunakan oleh jaringan e-mail yang berbasis Microsoft Exchange, Lotus Domino, dan Novell Group Wise. Khusus pada pengguna individu, mereka dapat menggunakan layanan e-mail nirkabel yang disediakan oleh provider tanpa harus menginstalasi BES. Para pengguna individu dapat menggunakan BlackBerry Internet Solution tanpa harus menginstalasi BES di smartphone mereka. BES memang ditujukan bagi pelanggan korporasi dengan cakupan usaha yang besar. Perangkat lunak ini mengintegrasikan seluruh smartphone BlackBerry pada suatu organisasi dengan sistem perusahaan yang telah ada.

Keuntungan yang diperoleh adalah memperluas komunikasi nirkabel dan data perusahaan kepada pengguna aktif dengan cara yang aman. Karena pada BES ini, RIM menyediakan fitur end-to-end encryption didalamnya. Fitur enkripsi yang disediakan pada BES ini menggunakan algoritma AES dan 3DES didalamnya. Fitur ini memungkinkan sebuah perusahaan untuk memiliki sebuah *master key*, dimana key ini nantinya akan digunakan untuk mengenkripsi semua proses komunikasi data yang ada di perusahaan tersebut, selain itu, PIN sender dan PIN receiver juga dapat dijadikan parameter dalam melakukan pengenkripsian data, dimana algoritma yang digunakan adalah algoritma *scrambling* yang akan mengacak PIN hexadecimal tersebut untuk mengenerate sebuah key.[7]

BlackBerry Professional Software (BPS)

BPS merupakan komunikasi nirkabel dan kolaborasi solusi bagi usaha kecil dan menengah. Ia menghadirkan berbagai fitur yang dibutuhkan karyawan, dalam sebuah paket yang mudah dipasang dan harga yang lebih murah.

BlackBerry Internet Service (BIS)

Perangkat lunak yang diperuntukkan bagi pengguna pribadi ini memungkinkan Anda untuk mengintegrasikan smartphone dengan 10 akun e-mail yang berbasis Post Office Protocol (POP3) dan Internet Message Access Protocol (IMAP), menerima dan mengirim pesan instan, serta berselancar di internet. Dengan BIS, kita juga dapat membuka tambahan data (attachment) dalam bentuk excel, word, powerpoint, pdf, zip, jpg, gif dengan tingkat kompresi data yang tinggi. Dalam menggunakan servisnya, BIS pada Blackberry sama sekali tidak menggunakan fitur end-to-end message encryption.[8]

BlackBerry Mobile Data System (BlackBerry MDS)

Sebuah aplikasi optimisasi pengembangan kerangka kerja untuk BlackBerry Enterprise Solution, menyediakan Anda sebuah alat pengembangan untuk membangun, menyebarluaskan, serta mengatur interaksi antara BlackBerry smartphone dan aplikasi perusahaan.

Jaringan Seluler

Smartphone BlackBerry dapat beroperasi pada berbagai jaringan seluler berikut, yaitu:

CDMA2000 1X Ev-DO

Jaringan CDMA2000 1X memungkinkan kita untuk memelihara koneksi jaringan nirkabel untuk layanan data. Jaringan ini menyokong layanan untuk data berkecepatan-tinggi, dirancang untuk komunikasi data di area luas serta menawarkan layanan suara berkualitas tinggi, didukung oleh Ev-DO (Evolution Data Optimized) atau Evolusi Optimalisasi Data. Operator CDMA di Indonesia yang sudah mengoperasikan jaringan CDMA2000 1X Ev-DO yakni Telkom Flexi, Mobile-8, dan Smart Telecom. Telkom adalah operator pertama di Indonesia yang mengoperasikan jaringan ini di Surabaya. Teknologi terakhir baru mencapai Ev-DO Rev 0 yang mana kecepatannya baru mencapai 2,4 Mbps sedangkan Smart Telecom dan Mobile-8 sudah mencapai kecepatan 3,1 Mbps.

GSM/GPRS/EDGE/UMTS

Jaringan GSM / GPRS / EDGE / UMTS memungkinkan kita untuk memelihara koneksi virtual dengan jaringan nirkabel untuk layanan data. GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for Global Evolution) dan UMTS (Universal Mobile Telecommunications System) adalah sebuah jaringan paket yang bisa dipakai bergantian, dirancang untuk komunikasi data pada area luas, sementara GSM (Global System for Mobile Communications) memberikan layanan suara berkualitas tinggi. UMTS, atau biasa dikenal sebagai 3GSM, memberikan sinkronisasi suara dan fungsionalitas data, memberikan dukungan bagi perpindahan data dengan kecepatan tinggi.

Wireless Local Area

Wireless Local Area Networks (WLAN) beroperasi pada frekuensi yang tidak memiliki izin dan biasanya digunakan untuk mengalihkan kemacetan jaringan perusahaan di udara. Hal ini diperlukan untuk meminimalkan kebutuhan akan jaringan LAN yang tradisional. WLAN dirancang dengan tujuan agar departemen IT bisa mengatur jaringan nirkabel mereka sendiri, memungkinkan mobilitas internal bagi fasilitas yang diperuntukkan bagi karyawan perusahaan. Dengan adanya Voice over IP (VoIP), WLANs kini bisa digunakan untuk

menghantarkan data maupun suara.

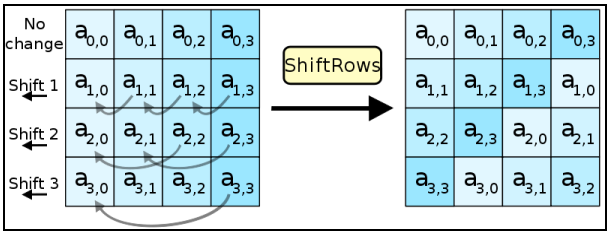
III.II Algoritma Enkripsi AES dan 3DES

Advanced Encryption Standard (AES)

Dalam kriptografi, Advanced Encryption Standard (AES) merupakan standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok cipher, yaitu AES-128, AES-192 and AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES).

AES diumumkan oleh Institut Nasional Standar dan Teknologi (NIST) sebagai Standar Pemrosesan Informasi Federal (FIPS) publikasi 197 (FIPS 197) pada tanggal 26 November 2001 setelah proses standarisasi selama 5 tahun, di mana ada 15 desain enkripsi yang disajikan dan dievaluasi, sebelum Rijndael terpilih sebagai yang paling cocok. AES efektif menjadi standar pemerintah Federal pada tanggal 26 Mei 2002 setelah persetujuan dari Menteri Perdagangan. AES tersedia dalam berbagai paket enkripsi yang berbeda. AES merupakan standar yang pertama yang dapat diakses publik dan sandi-terbuka yang disetujui oleh NSA untuk informasi rahasia.

Rijndael dikembangkan oleh dua kriptografer Belgia, Joan Daemen dan Vincent Rijmen, dan diajukan oleh mereka untuk proses seleksi AES. Rijndael (diucapkan [rɛinda:l]) adalah permainan kata dari kedua nama penemu.



Gambar 2 : Proses shift dalam AES

Ada 10, 12, atau 14 putaran (round) dalam AES. Jumlah kitaran ini sesuai dengan ukuran kunci yang digunakan.

Setiap kitaran mengandungi:

Penggantian Byte yang sama seperti DES

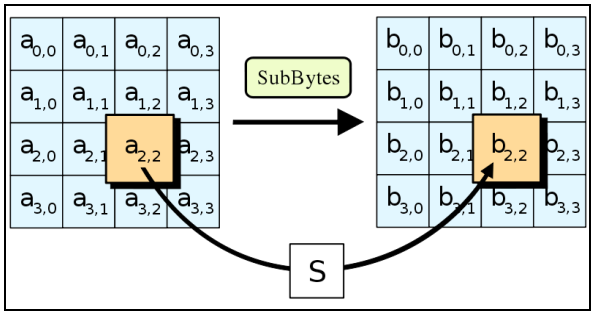
Peralihan = Pertukaran baris

Campur Jalur = Peralihan Kiri & XOR Bit-bit.

Penambahan Subkunci = XOR Bagian Kunci dengan Keputusan Kitaran [9]

3DES (Triple Data Encryption Standard)

Dalam bidang kriptografi, Data Encryption Standard (DES) adalah sebuah algoritma enkripsi sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit.



Gambar 3: Ilustrasi substitusi bytes pada DES

DES untuk saat ini sudah dianggap tidak aman lagi. Penyebab utamanya adalah ukuran kuncinya yang sangat pendek (56-bit). Sejak beberapa tahun yang lalu DES telah digantikan oleh Advanced Encryption Standard (AES). [10]

3DES (Triple Data Encryption Standard) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma 3DES adalah suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Perbedaan DES dengan 3DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu kunci yang panjangnya 56-bit, sedangkan pada 3DES menggunakan 3 kunci yang panjangnya 168- bit (masing-masing panjangnya 56-bit). Pada 3DES, 3 kunci yang digunakan bisa bersifat saling bebas (K1 , K2 , K3) atau hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1 , K2 dan K3 = K1). Karena tingkat kerahasiaan algoritma 3DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma 3DES dianggap lebih aman dibandingkan dengan algoritma DES. [11]

IV. ANALISIS MASALAH

Penulis akan menganalisis permasalahan ini berdasarkan sudut pandang bahwa Pemerintah Indonesia yang diwakili oleh Menkominfo-nya (Menteri Komunikasi dan Informasi Negara) Tifatul Sembiring memberikan tuntutan ke RIM karena fitur enkripsinya yang membuat pemerintah Indonesia tidak dapat menyadap proses komunikasi entitas kejahatan di Indonesia, antara lain kejahatan korupsi dan kejahatan terorisme.

Poin pertama yang ingin penulis analisis adalah poin enkripsi dari Blackberry Messenger itu sendiri. Sebelum itu, penulis ingin menekankan bahwa fitur enkripsi yang disediakan oleh Blackberry adalah fitur yang diperuntukkan khusus untuk pelanggan BES (Blackberry Enterprise Server), sedangkan BIS

(Blackberry Internet Service) tidak menyediakan fitur enkripsi pada defaultnya. BBM menggunakan dua tipe enkripsi yang diimplementasi. Implementasi pertama menggunakan algoritma AES, yang kedua menggunakan algoritma 3DES. Untuk algoritma AES, key yang digunakan adalah masterkey dari enterprise. Sedangkan untuk algoritma 3DES, key yang digunakan adalah PIN sender, PIN user, dan masterkey dari enterprise. Karena pada 3DES ada 3 key yang digunakan.

Implementasi enkripsi tersebut secara tidak langsung menstate bahwa tanpa mengetahui masterkey dari enterprise, maka pesan-pesan data yang dikirimkan lewat data server BES tidak akan dapat dipecahkan. Karena dalam keberjalanannya sekarang, algoritma AES dan 3DES masih tergolong ampuh dan belum ada solusi pemecahan ataupun kelemahan yang dapat dijelaskan secara eksplisit.

Untuk penggunaannya di Indonesia, sebenarnya mayoritas warga Indonesia menggunakan paket BIS dari BBM, bukan BES. Oleh karena itu, secara default tidak ada proses enkripsi yang ditawarkan oleh Blackberry pada saat pengiriman pesan. Enkripsi data terjadi saat pengiriman data oleh carrier atau provider BIS yang digunakan oleh handheld Blackberry tersebut. Jadi, untuk paket BIS, apabila ingin dilakukan pengecekan log pengiriman pesan atau data, cukup merequestnya dari provider atau carrier yang digunakan dari handheld yang bersangkutan, karena tidak ada fitur enkripsi yang ditawarkan dari Blackberry apabila menggunakan paket BIS. Maka untuk penggunaan paket BIS, Blackberry dapat dinyatakan aman untuk digunakan di Indonesia, karena data dan pesan yang dikirim lewat Blackberry dapat direquest untuk dicatat via carrier atau provider internetnya.

Untuk penggunaan paket BES, fitur enkripsi dijalankan lewat dua metode yang sudah dianalisis di atas. Dalam penggunaannya, BES dapat dikatakan sangat aman dan bahkan menurut sumber yang ada pada artikel diatas, data yang dikirim lalu lalang pun tidak dapat diakses oleh pemerintah sekalipun. Hal ini disebabkan oleh masterkey yang dimiliki oleh sebuah perusahaan itu tidak dishare ke pemerintah, sementara PIN sender dan PIN user itu masih bisa dilacak oleh pemerintah. Karena kedua algoritma enkripsi pada BES yaitu AES dan 3DES kedua-duanya menggunakan masterkey sebagai kunci untuk proses pengenkripsian, maka BES dapat dikatakan aman.

Untuk penggunaannya di Indonesia, BES dapat digunakan servisnya oleh perusahaan-perusahaan yang membutuhkan fitur pengelolaan data dan pesan secara terstruktur misalkan menggunakan Microsoft Exchange, disini Blackberry dapat menjadi sumber komunikasi pesan dan data dalam jaringan perusahaan tersebut. Sejauh ini, penggunaan BES di Indonesia dapat dikatakan cukup jarang. Meskipun demikian, jikalau ada perusahaan yang menggunakannya, dapat disimpulkan suatu statement bahwa sangat memungkinkan jika perusahaan tersebut dapat menggunakan fitur enkripsi data dan pesan agar proses komunikasi didalamnya tidak dapat disadap (karena set default enkripsi untuk BES adalah NOT ENCRYPTED).

Karena fitur enkripsi pada paket BES yang sangat aman ini, proses kejahatan dapat dilakukan via BBM di paket BES ini. Sebuah perusahaan dapat mendaftarkan karyawan-karyawan perusahaannya untuk masuk ke dalam jaringan enterprisenya yang menggunakan paket BES tersebut. Maka kemungkinan kumpulan karyawan ataupun atasan perusahaan adalah pelaku kejahatan tetap ada.

Solusi untuk permasalahan ini adalah dengan menerapkan prosedur khusus untuk pengguna BES, bukan dengan menarik peredaran Blackberry dari masyarakat, karena itu merupakan solusi yang kurang cerdas menurut saya. Dengan menetapkan sebuah prosedur dalam penggunaan BES di sebuah perusahaan, pemerintah dapat memantau proses kejahatan jika dianggap salah satu atau beberapa anggota dari perusahaan tersebut adalah pelaku kejahatan. Prosedur ini dapat berupa pernyataan khusus dari pemerintah atau lewat perjanjian tiga pihak antara pemerintah dengan perusahaan dan Blackberry. Maka untuk penggunaan paket BES, Blackberry dapat dinyatakan aman untuk digunakan di Indonesia dengan syarat adanya prosedur yang memungkinkan pemerintah dapat merequest log pesan dari perusahaan atau menerima masterkey layanan BES dari perusahaan.

V. KESIMPULAN DAN SARAN

Dari serangkaian analisis yang telah dilakukan oleh penulis, penulis dapat menyimpulkan beberapa hal, antara lain:

1. Ada dua paket Blackberry yang disediakan di Indonesia yaitu paket BIS dan BES.
2. Untuk penggunaan paket BIS, Blackberry Messenger aman digunakan di Indonesia, karena tidak ada proses enkripsi yang ditawarkan oleh handheld Blackberry untuk paket BIS.
3. Untuk penggunaan paket BES, Blackberry Messenger aman digunakan di Indonesia, dengan syarat adanya prosedur yang memungkinkan pemerintah dapat merequest log pesan dari perusahaan atau menerima masterkey layanan BES dari perusahaan.

Dan berdasarkan kesimpulan tersebut, penulis ingin memberikan beberapa kontribusi berupa saran terutama kepada masyarakat yang belum tahu benar fungsi enkripsi pada Blackberry yang digunakan secara umum di Indonesia saat ini. Saran tersebut antara lain:

1. Untuk pemerintah, khususnya pihak-pihak terkait insiden isu pencabutan Blackberry ini, diharapkan lebih dalam saat mengkaji suatu permasalahan sebelum mengeluarkan statement yang dapat membuat panik masyarakat.

2. Untuk pemerintah, dalam hal ini Kementrian Komunikasi dan Informasi, jika ingin mendapatkan data komunikasi suatu pelaku kejahatan yang dilakukan via Blackberry, untuk paket BIS, dapat dilakukan dengan merequest lognya ke carrier atau provider internet service dari pelaku kejahatan yang terkait. Untuk paket BES, dapat dibuat prosedur yang memungkinkan pemerintah dapat merequest log pesan dari perusahaan atau menerima masterkey layanan BES dari perusahaan.
3. Untuk masyarakat, layanan BIS dan BES sebenarnya hanya fitur yang mempermudah komunikasi antara sebuah entitas masyarakat, sebaiknya tidak dipergunakan untuk tindak laku kejahatan, selain merisaukan pemerintah, jika banyaknya pelaku kejahatan via Blackberry nantinya semakin meningkat, bukan tidak mungkin Blackberry akan benar-benar dicabut peredarannya dari Indonesia.

DAFTAR PUSTAKA

[1] *http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/07/05/data-encryption-is-reason-for-blackberry-and-skype-ban-in-india.aspx* . Tanggal akses : 22 Maret 2011.
[2] http://nasional.inilah.com/read/detail/1128922/blokir-blackberry-tifatul-misleading . Tanggal akses : 22 Maret 2011.
[3] http://www.jpnn.com/read/2011/01/10/81508/Blokir-Blackberry-Sudah-Harga-Mati- . Tanggal akses : 22 Maret 2011.
[4] http://teknologi.inilah.com/read/detail/1138722/pemerintah-minta-kunci-enkripsi-data-blackberry . Tanggal akses : 22 Maret 2011.
[5] http://www.bgr.com/2010/08/02/rim-your-blackberry-data-is-secure-even-from-governments/ . Tanggal akses : 22 Maret 2011.
[6] http://id.wikipedia.org/wiki/Blackberry . Tanggal akses : 22 Maret 2011.
[7] http://en.wikipedia.org/wiki/BlackBerry . Tanggal akses : 22 Maret 2011.
[8] http://www.techjunoon.com/what-information-is-encrypted-on-your-blackberry/ . Tanggal akses : 22 Maret 2011.
[9] http://id.wikipedia.org/wiki/AES . Tanggal akses : 22 Maret 2011.
[10] http://id.wikipedia.org/wiki/Data_Encryption_Standard . Tanggal akses : 22 Maret 2011.
[11] http://pustaka.unpad.ac.id/archives/16781/ . Tanggal akses : 22 Maret 2011.
[12] Blackberry corp. 2010.*"BlackBerry_Internet_Service-Security_Feature_Overview--787371-0205030634-001-3.0-US"*. http://docs.blackberry.com . Tanggal akses : 2 Maret 2011.
[13] Blackberry corp. 2010.*"BlackBerry_Messenger-Security_Note--1325047-1020110747-001-US"*. http://docs.blackberry.com . Tanggal akses : 2 Maret 2011.
[14] Blackberry corp. 2010.*" FTO_D_Gold"*. http://docs.blackberry.com . Tanggal akses : 2 Maret 2011.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 22 Maret 2011
ttd

Jonathan Ery Pradana
13508007