Keamanan Peminjaman Buku Digital di Perpustakaan

Prisyafandiafif Charifa (13509081)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
prisyafandiafif.charifa@gmail.com

ABSTRAK

***E-book* merupakan teknologi yang banyak diminati oleh berbagai kalangan. *E-book* ini memiliki banyak keuntungan baik dari segi *provider* maupun konsumen. Dari sudut pandang *provider*, *E-book* dapat didistribusikan dan dipublikasikan dalam jangkauan yang luas dengan cara yang efisien dan sangat ekonomis. Dari sudut pandang konsumen, mereka bisa mendapatkan buku secara cepat tanpa harus menunggu ada kiriman barang dan konsumen dapat membacanya dimanapun baik itu *notebook*, *smartphone*, PDA, dll. Hal inilah yang mendorong adanya perpustakaan digital dimana buku yang ada pada perpustakaan digital ini adalah buku digital bukan berupa buku fisik. Namun untuk mengamankan buku digital yang ada pada perpustakaan dari tindak penduplikasian dan pendistribusian dari orang yang meminjam buku digital merupakan masalah utama yang dihadapi oleh perpustakaan digital. Tulisan ini menerangkan standar *E-book*, arsitektur aplikasi serta mekanisme keamanannya menyangkut DRM, EBX, dsb.**

***Kata Kunci*—keamanan, DRM, EBX, *E-book*, perpustakaan.**

I. PENDAHULUAN

Dalam arti tradisional, perpustakaan adalah sebuah koleksi buku dan majalah. Perpustakaan dapat juga diartikan sebagai kumpulan informasi yang bersifat ilmu pengetahuan, hiburan, rekreasi, dan ibadah yang merupakan kebutuhan hakiki manusia[1]. Walaupun dapat diartikan sebagai koleksi pribadi perseorangan, namun perpustakaan lebih umum dikenal sebagai sebuah koleksi besar yang dibiayai dan dioperasikan oleh sebuah kota atau institusi, dan dimanfaatkan oleh masyarakat yang rata-rata tidak mampu membeli sekian banyak buku atas biaya sendiri.

Namun, dengan koleksi dan penemuan media baru selain buku untuk menyimpan informasi, banyak perpustakaan dewasa ini juga berfungsi sebagai tempat penyimpanan dan/atau akses ke peta, mikrofilm, mikrofiche, *audio tape*, CD, LP, *video tape* dan DVD, dan menyediakan fasilitas umum untuk mengakses CD-ROM dan internet.

Perpustakaan dapat juga diartikan sebagai kumpulan informasi yang bersifat ilmu pengetahuan, hiburan, rekreasi, dan ibadah yang merupakan kebutuhan hakiki manusia.

Oleh karena itu perpustakaan modern telah didefinisikan kembali sebagai tempat untuk mengakses informasi dalam format apa pun, apakah informasi itu disimpan dalam gedung perpustakaan tersebut atau tidak. Dalam perpustakaan modern ini selain kumpulan buku tercetak, sebagian buku dan koleksinya ada dalam perpustakaan digital (dalam bentuk data yang bisa diakses lewat jaringan komputer).

Perpustakaan merupakan upaya untuk memelihara dan meningkattkan efisiensi dan efektifitas proses belajar-mengajar. Perpustakaan yang terorganisasi secara baik dan sisitematis, secara langsung atau pun tidak langsung dapat memberikan kemudahan bagi proses belajar mengajar di sekolah tempat perpustakaan tersebut berada[1]. Hal ini, terkait dengan kemajuan bidang pendidikan dan dengan adanya perbaikan metode belajar-mengajar yang dirasakan tidak bisa dipisahkan dari masalah penyediaan fasilitas dan sarana pendidikan.

Perpustakaan digital adalah perpustakaan yang mempunyai koleksi buku sebagian besar dalam bentuk format digital dan yang bisa diakses dengan komputer[1]. Jenis perpustakaan ini berbeda dengan jenis perpustakaan konvensional yang berupa kumpulan buku tercetak, film mikro (*microform* dan *microfiche*), ataupun kumpulan kaset audio, video, dll. Isi dari perpustakaan digital berada dalam suatu komputer *server* yang bisa ditempatkan secara lokal, maupun di lokasi yang jauh, namun dapat diakses dengan cepat dan mudah lewat jaringan komputer.

Istilah perpustakaan digital pertama kali diperkenalkan lewat proyek NSF/DARPA/NASA: Digital Libraries Initiative pada tahun 1994[6]. Perpustakaan digital yang paling banyak dikenal saat ini adalah Proyek Gutenberg, ibiblio dan Internet Archive, serta proyek yayasan Wikimedia seperti Wikisource, Wikipedia, Wiktionary, Wikiquote, Wikibooks, Wikinews, Wikispecies, Wikiversity, Commons, Meta-Wiki, MediaWiki, dll.

Pada perpustakaan digital buku-buku yang berupa fisik seperti kertas diganti oleh buku elektronik. Buku elektronik (biasa disebut *e-book*) atau buku digital adalah versi elektronik dari buku. Jika buku pada umumnya terdiri dari kumpulan kertas yang dapat berisikan teks atau gambar, maka buku elektronik berisikan informasi digital yang juga dapat berwujud teks atau gambar. Dewasa ini

buku elektronik diminati karena ukurannya yang kecil bila dibandingkan dengan buku, dan juga umumnya memiliki fitur pencarian, sehingga kata-kata dalam buku elektronik dapat dengan cepat dicari dan ditemukan[1]. Terdapat berbagai format buku elektronik yang banyak digunakan. Popularitas umumnya bergantung pada ketersediaan berbagai buku elektronik dalam format tersebut dan kemudahan akses piranti lunak yang digunakan untuk membaca jenis format tersebut. Format tersebut tersedia dalam bentuk berkas teks polos, PDF, JPEG, LIT, *Open Electronic Book Package*, dan HTML[1]. Masing-masing format memiliki kelebihan dan kekurangan masing-masing, yang juga bergantung dari perangkat yang digunakan untuk membaca buku elektronik tersebut.

Salah satu usaha untuk melestarikan literatur berbentuk buku yang banyak jumlahnya dan memerlukan biaya perawatan yang mahal adalah dengan melakukan konversi dari bentuk buku fisik ke bentuk buku elektronik. Dalam hal ini akan banyak ruang dan juga usaha yang dihemat untuk merawat literatur-literatur tersebut.

Saat ini sumber buku elektronik yang legal di Indonesia belumlah banyak, antara lain dirilis oleh Departemen Pendidikan Nasional (kini menjadi Kementerian Pendidikan Nasional) dengan dibukanya Buku Sekolah Elektronik (BSE). BSE adalah buku elektronik legal dengan lisensi terbuka yang meliputi buku teks mulai dari tingkatan dasar sampai lanjut. Buku-buku di BSE telah dibeli hak ciptanya oleh pemerintah Indonesia melalui Depdiknas, sehingga bebas diunduh, direproduksi, direvisi serta diperjualbelikan tetapi dengan batas atas harga yang telah ditentukan. Lebih dari itu, seluruh buku ini telah dinilai dan lolos saringan dari penilai di Badan Nasional Standardisasi Pendidikan (BNSP).

Kebijakan Depdiknas waktu itu adalah membeli hakcipta 95 judul buku teks pelajaran SD/Madrasah Ibtidaiyah, 72 judul buku teks SMP/Madrasah Tsanawiyah, 24 judul buku teks SMA/ Madrasah Aliyah dan 216 judul buku teks SMK. Buku-buku itu meliputi pelajaran matematika, Bahasa Indonesia, IPA, Pendidikan Kewarganegaraan dan Ilmu Pengetahuan Sosial. Juga Bahasa Inggris, mata pelajaran adaptif, mata pelajaran produktif dan mata pelajaran normatif untuk jenjang SMK. Secara keseluruhan terdapat 407 judul buku.

Lembaga Ilmu Pengetahuan Indonesia (LIPI) juga menyediakan sarana bagi penulis untuk membuka akses pada aneka buku elektronik dengan lisensi terbuka. Sarana ini telah dibuka dengan nama BUKU-e. Selain untuk buku-buku ilmiah, BUKU-e LIPI juga ditujukan untuk buku 'pembelajaran ilmiah', seperti diktat, buku teks, dll. Termasuk buku-buku BSE juga termasuk dalam BUKU-e LIPI.

Saat ini, dunia industri mulai melirik *e-book*. Penerbit Mizan misalnya, pada tahun 2001 mempelopori keberadaan buku digital dengan memberikan *e-book* berjudul "Wasiat Sufi Imam Khomeini kepada Putranya Ahmad Khomeini" secara gratis di situs mereka. Untuk memperkenalkan *e-book* pada masyarakat, beberapa pengusaha mencoba menggabungkan buku elektronik dengan bisnis toko buku di internet, meniru Amazon. Sebagai contohnya adalah E-Book Centro yang dapat diakses melalui situs ebook-centro.com.

Tidak bisa dipungkiri memang keberadaan buku elektronik ini menjadi suatu masalah bagi perpustakaan digital. Karena sifat perpustakaan adalah meminjamkan buku pada seseorang dengan periode waktu tertentu dan ketika waktu peminjaman buku tersebut telah habis maka peminjam harus mengembalikan buku pada perpustakaan dan jika melebihi batas waktu peminjaman buku maka orang yang meminjam buku tersebut akan dikenai sanksi berupa denda.

Jika kita lihat sifat buku digital yang mudah di duplikasikan berbeda dengan buku biasa maka hal inilah yang menjadi masalah. Bagaimana caranya agar perpustakaan digital yang meminjamkan buku digital ini kepada para peminjam dapat menggunakan aturan-aturan yang ada seperti pada perpustakaan konvensional. Bagaimana sistem pengamanan dari pencurian buku digital. Makalah ini akan membahas lebih lanjut mengenai hal-hal tersebut.

II. DASAR TEORI

II.1 Ruang Lingkup Keamanan Buku Digital

E-book merupakan suatu aset yang ada dalam format digital[2]. Dalam penjualannya *e-book* harus aman untuk disimpan, dikirim, dan digunakan terhadap duplikasi dan distribusi. Bisnis di bidang *e-book* dilakukan melalui sistem DRM untuk *e-book*. Sebuah sistem DRM yang utama adalah terdiri dari *e-book server*, *reading systems*, dan fasilitas transmisi. Dalam sistem DRM, isi dan informasi terkait yang ada pada *e-book* disimpan dalam *e-book server* dan/atau *e-book reading system* dan transmisi utama dilakukan melalui internet. Untuk menjaga *e-book* bebas dari duplikasi dan distribusi, kita harus membuat tempat penyimpanan *e-book* dan menjamin proses transmisi aman, sebagai contoh yaitu dengan membuat sistem *E-book* bebas dan aman terhadap duplikasi dan distribusi. Jadi disini dapat didefinisikan bahwa keamanan *e-book* adalah bagaimana menjaga sistem kemanan *e-book* dan membatasi duplikasi dan distribusi *e-book*.

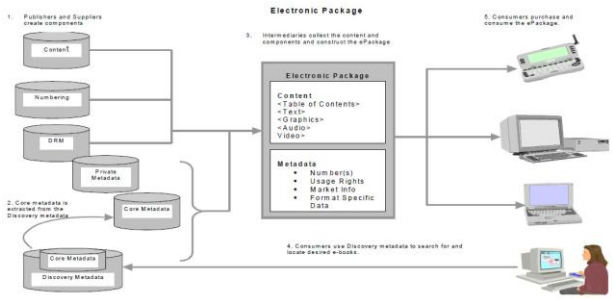
II.2 *Digital Rights Managements* (DRM) untuk *E-book*

DRM (*Digital Rights Managements*) dikembangkan oleh Asosiasi Penerbit Amerika. Asosiasi Penerbit Amerika meliputi partisipan dari pihak penerbit maupun industri *e-commerce*. DRM untuk *e-book* ini dimaksudkan untuk mempromosikan penggunaan *e-book* dan untuk memfasilitasi para pengembang *e-book* yang terkait teknologi. DRM untuk *e-book* menentukan fungsi dari sistem DRM, dasar dari arsitektur aplikasi DRM, masalah interoperabilitas dari perbedaan solusi DRM dan persyaratan sistem DRM dalam aspek teknologi, perundang-undangan, Hak Asasi Spesifikasi Bahasa,

paket kontrol elektronik, format file dan kepercayaan infrastruktur. Hal ini bertujuan untuk menyediakan spesifikasi standar DRM yang berbeda untuk sistem pada penyedia *e-book*. Versi pertama dari DRM untuk *e-book* dirilis pada bulan Desember tahun 2000[2].

II.3 Model Aplikasi Tipikal DRM

Model aplikasi DRM diklasifikasikan sebagai model pasar *e-book* dan paket model *e-book*. Model pasar *e-book* membutuhkan sistem DRM yang mendukung semua kegiatan pada tahap penerbitan dari pasar *e-book*. Model ini mendefinisikan pasar *e-book* pada lima tahap termasuk membuat dan menerbitkan, memasarkan dan mendistribusikan, menjual kepada konsumen, mengkonsumsi konten dan konsumen dukungan. Penerapan sistem DRM harus mendukung semua kegiatan yang terlibat dalam fase ini. Model ini adalah sebuah bisnis model yang menggambarkan sistem DRM terutama dalam sudut pandang pasar. *E-book* model paket elektronik menggambarkan sistem DRM dari sudut pandang teknik, dan hal ini menentukan teknologi dasar untuk penerbitan, transmisi dan penggunaan isi *e-book* digital dalam sistem DRM.



Gambar 1. Model Paket *E-book*[2]

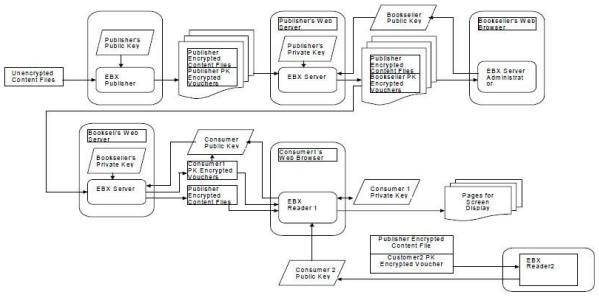
II.4 Sistem Elektronik *Book Exchange* (EBX)

Sistem EBX sedang dikembangkan oleh kelompok EBX. Hal ini mendefinisikan cara mengamankan distribusi *e-book* dari penerbit ke penjual buku, dari penjual buku untuk konsumen, antara konsumen, dan antara konsumen dan bekerja sama[3]. Pada bagian ini, kita akan membahas fungsi dan masalah keamanan komputer sistem EBX.

Sistem EBX ditentukan dalam dua model, model fungsional dan model kepercayaan (*trust model*). Berdasarkan fungsi dari komponen sistem dan interaksi dari komponen yang terpercaya di sistem masing-masing, digambarkan seperti di bawah ini:

II.4.1 Model Fungsional

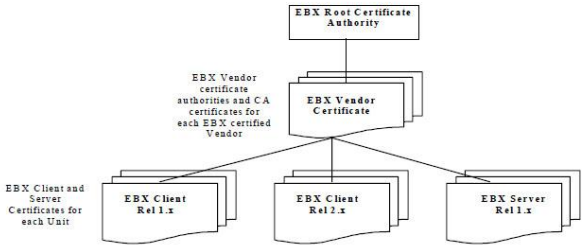
Model ini mendefinisikan sistem EBX dalam urutan mulai dari membuat, menerbitkan, distribusi hingga pindah ke tangan konsumen.



Gambar 2. Model Fungsional EBX[3]

II.4.1 Model Kepercayaan

Seperti yang telah disebutkan dalam model fungsional, sistem membaca EBX dan *server* terdiri dari jaringan EBX. Jaringan EBX ini terdiri dari dua komponen dari dua *vendor* yang berbeda. Selama dua komponen tersebut saling beroperasi, mereka perlu berkomunikasi dan menemukan apa kesamaan yang mereka miliki seperti algoritma enkripsi, panjang kunci, dan format dari file konten. Agar menjamin integritas jaringan secara keseluruhan dan menghindari memberikan informasi rahasia untuk penyerang potensial, setiap komponen yang terlibat dalam aktivitas komunikasi tersebut perlu saling percaya. Hal ini membutuhkan otentikasi bersama antara klien dan *server*. Mekanisme otentikasi tersebut adalah *Public Key Infrastructure* (PKI), yang melakukan identifikasi, sertifikasi, dan otentikasi fungsi yang diperlukan oleh setiap komponen. Keseluruhan arsitektur EBX *Certificate Authority* adalah seperti pada gambar di bawah ini:



Gambar 3. Arsitektur EBX *Certificate Authority*[3]

III. ANALISIS DAN PEMBAHASAN

III.1 Fungsionalitas dan Mekanisme Keamanan dari DRM

Berbeda dengan perdagangan buku fisik, *e-book* diperdagangkan utamanya melalui internet dengan teknologi digital. Pada proses jual beli *e-book*, dalam banyak kasus penjual dan pembeli tidak bertatap muka. Dapatkah mereka saling percaya? Bagaimana transaksi perdagangan dilakukan dengan aman? DRM menangani sebagian besar masalah keamanan untuk pasar E-book meskipun beberapa masalah masih ada.

DRM menyediakan konten digital yang dilindungi dengan enkripsi. Menurut teori DRM, dapat diketahui bahwa

sistem DRM akan mengenkripsi isi dan metadata dengan algoritma standar enkripsi simetris seperti DES, RC4, dll. DRM harus memungkinkan penerbit atau penulis untuk menentukan atau memilih algoritma enkripsi yang berbeda dan panjang kunci yang berbeda pula[3]. Sebagai contoh, suatu penerbit menggunakan suatu kakas DRM khusus untuk mengenkripsi judul *e-book* secara acak dengan satu kunci enkripsi sehingga terciptalah *voucher* untuk judul *e-book* tersebut. Selama proses distribusi, voucher didekripsi dengan kunci privat penerbit pertama, kemudian dienkripsi dengan kunci publik konsumen dan diterima oleh konsumen tersebut.

Selain enkripsi, teknologi *digital watermarking* dapat digunakan, meskipun teknologi ini tidak dapat mencegah akses yang tidak terotentifikasi ke masing-masing *e-book*. Walaupun begitu, teknologi *digital watermarking* dapat digunakan untuk melacak dan mencegah distribusi yang tidak sah dan ilegal.

E-book merupakan suatu aset yang ada dalam format digital[2]. Dalam penjualannya *e-book* harus aman untuk disimpan, dikirim, dan digunakan terhadap duplikasi dan distribusi. Bisnis di bidang *e-book* dilakukan melalui sistem DRM untuk *e-book*. Sebuah sistem DRM yang utama adalah terdiri dari *e-book server*, *reading systems*, dan fasilitas transmisi. Dalam sistem DRM, isi dan informasi terkait yang ada pada *e-book* disimpan dalam *e-book server* dan/atau *e-book reading system* dan transmisi utama dilakukan melalui internet. Untuk menjaga *e-book* bebas dari duplikasi dan distribusi, kita harus membuat tempat penyimpanan *e-book* dan menjamin proses transmisi aman, sebagai contoh yaitu dengan membuat sistem *E-book* bebas dan aman terhadap duplikasi dan distribusi. Jadi disini dapat didefinisikan bahwa keamanan *e-book* adalah bagaimana menjaga sistem kemanan *e-book* dan membatasi duplikasi dan distribusi *e-book*.

III.2 "Celah" pada Keamanan E-book

Saat ini, banyak penerbit dan penyedia *e-book* melakukan bisnisnya melalui internet. Pasar *e-book* yang besar dan terus berkembang telah mendorong munculnya banyak penerbit atau penyedia *e-book* tersebut. Perangkat lunak pembaca *e-book* yang paling populer saat ini adalah Adobe PDF dan Acrobat Microsoft Reader[4]. Walaupun begitu, tidak menjamin bahwa dua perangkat lunak tersebut memiliki fitur keamanan yang baik.

Kriptanalis dari Rusia bernama Dimitry Sklyarov pernah memaparkan mekanisme keamanan perangkat lunak Adobe Acrobat untuk membaca *e-book* yang dilihat dari sudut pandang pembaca beserta kelemahan apa saja yang ditemukan dari perangkat lunak Adobe Acrobat tersebut dalam suatu konferensi DEF CON 9 pada tanggal 13 Juli 2001[4].

Dalam sistem DRM untuk *e-book* dari Adobe, enkripsi berkas dan manajemen kunci ditangani oleh *plug-in* yang dikembangkan oleh pihak ketiga, yang mana *plug-in* tersebut meliputi *Standard security handler*, ROT13 *security handler*, *FileOpen security handler*, dan *SoftLock security handler*. Seperti yang diketahui, perangkat lunak pembaca Adobe PDF mendapatkan kunci untuk enkripsi suatu dokumen dari sebuah *security handler* dan kemudian mendekrip isi dari *e-book* tersebut[4]. Karena itulah, algoritma kriptografi yang digunakan dalam suatu *security handler* sangat menentukan tingkat keamanan dari sistem DRM untuk *e-book* dari Adobe. Sayangnya, semua *security handler* yang digunakan untuk sistem DRM tersebut memiliki "celah" di keamanannya, menurut Sklyarov.

Standard security handler menggunakan RC4 *stream cipher* untuk mengenkripsi isi dari suatu berkas PDF dengan menggunakan kunci enkripsi yang unik. Kunci enkripsi tersebut dienkrip dan nantinya akan disimpan di dalam berkas PDF. Dengan kata lain, semua orang yang memiliki akses ke berkas PDF tersebut, baik itu pemilik kunci enkripsi atau sekadar pengguna kunci enkripsi, dapat memperoleh kunci enkripsinya dengan menggunakan teknik-teknik kriptanalisis sederhana, dan bila sudah didapatkan kuncinya, maka orang tersebut dapat mendekripsi isi berkas PDF tersebut.

ROT13 *security handler* juga sudah terbukti cukup lemah keamanannya. Cara kerjanya adalah dengan mengenkripsi semua dokumen dengan kunci enkripsi yang tetap. Kunci enkripsi ini juga disimpan di dalam *plug-in*, sehingga dapat ditemukan dengan mudah[5].

FileOpen security handler menggunakan bermacam-macam kunci enkripsi, namun segala hal yang digunakan untuk menentukan kunci-kunci tersebut disimpan di dalam berkas PDF yang terenkripsi. Menurut pengalaman, *attackers* dapat dengan mudah menemukan kunci-kunci enkripsi tersebut[5].

Sedangkan untuk *Softlock security handler* juga dapat dengan mudah dipecahkan dengan suatu cara, menurut Dimitri Sklyarov[5].

Terlepas dari segala "celah" yang dijelaskan sebelumnya, dewasa ini telah ada suatu perangkat lunak bernama *Advanced Ebook Password Remover* (AEBPR) yang dipasarkan melalui internet oleh suatu perusahaan bernama ElcomSoft. AEBPR ini dapat menghilangkan mekanisme *password* yang dibutuhkan oleh pengguna untuk membaca *e-book*, baik itu *password* dari 128-bit RC4 atau yang lainnya. AEBPR juga bisa menghilangkan mekanisme keamanan yang diciptakan oleh *security handler* yang telah disebutkan sebelumnya[5].

Setelah masalah keamanan ini diketahui, perangkat lunak pembaca *e-book* Adobe Acrobat eBook Reader akhirnya diperbaharui. Perusahaan ElcomSoft dipaksa untuk berhenti memasarkan AEBPR oleh Tim Anti Pembajakan dari Adobe pada tanggal 25 Juni 2001. Ironisnya, Dimitri Sklyarov ditahan oleh kepolisian setelah konferensi DEF CON 9 karena dianggap telah melanggar *Digital Millenium Copyright Act* (DMCA)[6].

Selain adanya "celah" pada keamanan perangkat lunak pembaca *e-book* Adobe Acrobat eBook Reader seperti yang dijelaskan sebelumnya, ternyata diketahui juga bahwa perangkat lunak Microsoft eBook Reader juga mempunyai "celah" pada keamanannya. Sebuah program dekripsi dapat memecahkan sistem keamanan tingkat lima perangkat lunak Microsoft eBook Reader dan berhasil mengubah *e-book* menjadi suatu berkas biasa yang dapat dibuka pada berbagai *web browser*[5].

III.3 Kekuatan dan Kelemahan pada Sistem Keamanan E-book

Untuk menganalisis kekuatan dan kelemahan pada sistem keamanan *e-book*, perlu diketahui dulu mengenai empat jenis serangan (*attack*) yang sering diberikan pada suatu sistem keamanan, yaitu sebagai berikut:

III.3.1 Serangan pada *Content Server*

Jenis serangan ini memungkinkan untuk terjadinya pengaksesan dan pengubahan dari isi suatu berkas *e-book* yang terdapat di dalam *server* penerbit atau penjual *e-book*. Serangan ini juga memungkinkan terjadinya penolakan terhadap berbagai layanan (*service*). Untuk menanggulangi jenis serangan ini, terdapat langkah-langkah yang harus dilakukan untuk mengamankan sistem operasi dengan menggunakan *firewall*. Dari penjelasan sebelumnya, dapat diketahui bahwa dibutuhkan sistem *e-book* dalam lingkungan terdistribusi. Dalam sistem DRM untuk *e-book*, konsumen umumnya mendapatkan berbagai layanan akses melalui *server* penjual atau penerbit *e-book*. *Server* ini harus diberikan penanganan khusus seperti mengamankan sistem operasi dan menggunakan *firewall*. Ada baiknya jika komunikasi yang terjadi antara klien dan server tersebut berada di bawah kendali yang terotentikasi dan tersertifikasi. Semua informasi penting yang disimpan dan dikirim akan dienkripsi oleh *server*, sehingga keamanan pada *server* dalam sistem DRM ini sebenarnya cukup mudah untuk dilakukan, dan kemungkinan untuk ditembus atau dikalahkannya cukup kecil.

III.3.2 Serangan pada *Encrypted Content*

Serangan ini termasuk juga serangan yang memecahkan isi *e-book* yang terenkripsi sehingga *e-book* tersebut dapat dengan mudah didistribusikan kepada siapapun secara ilegal. Serangan ini adalah ancaman yang paling berbahaya pada sistem DRM. *Attacker* dapat dengan mudah mendapatkan informasi penting untuk membuat ulang kunci-kunci enkripsi. Pembuatan ulang kunci-kunci ini dapat dilakukan dengan menggunakan fasilitas komputasi yang mumpuni dengan usaha yang cukup masuk akal. Solusi yang dapat dilakukan untuk mencegah jenis serangan ini adalah dengan menggunakan teknologi kriptografi yang tepat sehingga akan semakin sulit bagi para *attacker* untuk membuat ulang kunci-kunci enkripsi.

III.3.3 Serangan pada *Reader System*

Reader system dewasa ini didistribusikan dalam lingkungan yang sangat luas dan berbeda. *Reader system* dapat digunakan untuk mendekrip dokumen. Seluruh atau sebagian informasi yang berhubungan dengan kunci enkripsi dari suatu *e-book* disimpan dalam perangkat *reader*. *Attacker* dapat dengan mudah mendapatkan informasi penting tersebut dengan melakukan *cracking* pada *reader system*. Serangan ini cukup susah untuk dicegah.

III.3.4 "Meniru" Pengguna atau Konsumen yang Sah

Dalam sistem DRM, mekanisme verifikasi dan otentifikasi dapat diimplementasikan untuk menjaga integritas jaringan. Mekanisme ini dapat membatasi peniruan, namun tidak dapat mencegahnya secara total. Setiap orang, tidak peduli apakah itu *attacker* atau bukan, dapat menjadi seorang konsumen yang sah.

Dari sudut pandang teknis, sistem *e-book* adalah sebuah sistem yang cukup rumit dan menyebar secara luas. Sejalan dengan itu, implementasi keamanan pada sistem ini sesungguhnya sangatlah sulit. Cara yang dapat dilakukan untuk meningkatkan keamanan *e-book* adalah dnegan menggunakan teknologi yang tepat dan mengimplementasikan *plug-in security handler* yang tepat.

IV. SIMPULAN

Seluruh organisai dan *vendor* penyedia *e-book* berusaha untuk mengatasi masalah keamanan dan membuat *reader system* kepemilikan mereka sempurna. Namun, dengan adanya kerumitan pada komunikasi dan distribusi, pembatasan teknologi, dan kuatnya serangan-serangan pada suatu sistem keamanan, dapat diketahui bahwa sebenarnya cukup mustahil untuk menutup semua "celah" pada keamanan *e-book* dari serangan-serangan yang ada. Beberapa contoh bukti yang pernah terjadi adalah seperti kasus terpecahkannya sistem keamanan dari perangkat lunak pembaca *e-book* Adobe Acrobat eBook Reader dan Microsoft eBook Reader.

Walaupun begitu, tetap saja *e-book* adalah suatu lahan bisnis yang baru muncul, dan untuk memastikan tingkat keamanan dari *e-book* benar-benar sempurna atau mendekati sempurna, masih dibutuhkan waktu yang tidak sedikit mulai dari sekarang. Dengan ditemukannya teknologi-teknologi enkripsi yang semakin sulit dipecahkan di masa depan tentu akan membantu dalam memastikan keamanan *e-book* ini.

Menggunakan teknologi kriptografi yang tepat adalah hal pertama yang harus diperhatikan dalam merancang dan mengimplementasi sistem DRM untuk *e-book*. Ancaman yang paling berbahaya untuk sistem DRM adalah serangan pada *encrypted content* yang memungkinkan *attacker* untuk membuat ulang kunci-kunci enkripsi sehingga isi dari *e-book* dapat didekrip dan didistribusikan secara ilegal. Ancaman kedua yang juga berbahaya adalah serangan pada *reader system*. Implementasi yang tepat pada *reader system* adalah kunci untuk menjaga

keamanan dari sistem DRM. Selain itu, juga diperlukan adanya pengawasan dan pelacakan yang terus menerus pada sistem keamanan *e-book* yang telah diimplementasikan. Hal ini penting agar organisasi atau vendor penyedia *e-book* dapat terus menemukan dengan cepat "celah" yang ada pada keamanan dan terus memperbaikinya.

V. DAFTAR PUSTAKA

[1] Fahmi, Ismail, 2004. Inovasi Jaringan Perpustakaan Digital: Network of Networks (NeONs). Makalah Seminar dan Workshop Sehari Perpustakaan dan Informasi Universitas Muhammadiyah Malang 4 Oktober 2004.

[2] Hasibuan, Zainal A, 2005. Pengembangan Perpustakaan Digital: Studi Kasus Perpustakaan Universitas Indonesia. Makalah Pelatihan Pengelola Perpustakaan Perguruan Tinggi. Cisarua - Bogor, 17-18 Mei 2005.

[3] Ikhwan, Arief, 2004. Konsep dan Perancangan dalam Outomasi Perpustakaan. Makalah Seminar dan Workshop Sehari Perpustakaan dan Informasi Universitas Muhammadiyah Malang 4 Oktober 2004.

[4] http://www.locklizard.com/ebook-security.htm
Tanggal Akses : 5 Mei 2013

[5] http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/ds-defcon/sld001.htm
Tanggal Akses : 10 Mei 2013

[6] http://loc.gov/copyright/legislation/dmca.pdf
Tanggal Akses : 10 Maret 2013

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, 20 Mei 2013

Prisyafandiafif Charifa
(13509081)