# Kriptografi pada Kehidupan Sehari-hari: Analisis Pengamanan dan Enkripsi Data pada Media Penyimpanan Portable

Aridarsyah Eka Putra
13507058
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
ariedz@students.itb.ac.id

**Abstract –Media penyimpanan adalah suatu device atau perangkat yang digunkan untuk merekam ataupun menyimpan informasi (data). Media penyimpanan bisa berisi informasi, proses informasi, ataupun keduanya. Sedangkan media penyimpanan portableadalah media penyimpanan yang mudah dibawa-bawa (arti portable dalam bahasa Indonesia). Pada makalah ini yang nantinya dimaksud dengan media penyimpanan portable adalah suatu device penyimpanan data digital (file citra, musik, video, dokumen, dsb) yang sering dibawa orang ketika bepergian untuk melakukan transfer data ke luar ataupun ke dalam device tersebut.**

**Pengamanan data adalah suatu cara untuk membuat data yang kita punya aman, aman di sini berarti hanya bisa diakses atau dipergunakan oleh orang-orang yang berhak atas data digital tersebut. Enkripsi adalah satu cara untuk melakukan pengamanan pada data.**

**Kata Kunci - enkripsi, media penyimpanan portable, pengamanan, solusi, teknologi.**

## I. PENDAHULUAN

Perkembangan zaman memang tak dapat diduga. Dewasa ini, kemajuan teknologi yang mengiringi perkembangan zaman sudah dapat dilihat nyata. Disamping itu, tuntutan era globalisasi untuk membuka kerjasama dengan negara-negara lain dalam melakukan usaha di negara-negara tertentu juga mempengaruhi perkembangan teknologi..

Penggunaan komputer secara personal (individu)maupun oleh perusahaan-perusahaan besar sudah bukan hal baru lagi. Untuk personal, penggunaan komputer secara umum banyak digunakan untuk mempermudah pengerjaan suatu tugas. Contohnya saja mahasiswa, boleh dibilang untuk zaman sekarang sudah sangat susah apabila seorang mahasiswa tidak mampu mengoperasikan komputer, hampir semua tugas diberikan membutuhkan komputer dalam pengerjaannya.

Namun untuk perusahaan, penggunaan komputer tersebut malah menjadi elemen wajib yang sudah tidak bisa terpisahkan dalamproses bisnis yang ada. Penggunaan komputer dilakukan untuk menjamin manajemen data dan informasi yang terintegrasi dan terjamin keamanannya. Sehingga, perusahaan-perusahaan tersebut dituntut untuk mengubah data-data analog sebelumnya menjadi data-data digital yang tersimpan di media penyimpanan (storage media) dalam komputer. Data yang tersimpan tersebut memerlukan pemeliharaan (maintenance) lebih lanjut agar kualitas dan keamanannya terjamin.

Seiring dengan perkembangan zaman tersebut, banyak orang yang sudah memanfaatkan media penyimpanan portable sebagai sarana untuk melakukan transfer data, contohnya flashdisk, hardisk eksternal, keping CD/DVD, SD CARD, memory stick, dll. Tentunya fenomena ini ada karena tuntutan efektifitas dan efisiensi yang akan membawa manusia ke peradaban maju dalam masa depan.

Peradaban yang ada pasti tidak selalu mulus berjalan seiring dengan zaman, tantangan pasti menghadang di semua aspek kehidupan manusia. Pernahkan kita bayangkan kalau kita menaruh barang berharga seperti emas atau berlian di tempat umum. Pastinya besar kemungkinan barang tersebut mengundang orang untuk mencurinya, tidak juga tertutup kemungkinan bahwa barang tersebut juga bisa benar-benar hilang dicuri. Barang berharga yang dimaksud tidak sebatas barang fisik yang memang harganya mahal bila dijual secara fisik di pasaran, tetapi punya makna yang cukup relatif tergantung orang menginterpretasikan barang berharga tersebut.

Sama halnya dengan data, mungkin beberapa dekade lalu (pada era perang dunia I dan II) data ataupun informasi adalah garis depan pertahanan dari suatu negara. Sangat penting bahwa transfer informasi yang dilakukan di suatu negara tidak sampai jatuh ke negara lain yang juga terlibat perperangan. Jika informasi jatuh pada negara yang kebetulan sedang berseteru maka akibatnya sangatlah fatal. Apalagi pada zaman teknologi informasi seperti sekarang, pengamanan data sangat lah penting, contohnya pada smartcard, telepon seluler, pay TV, dll. Saya di sini coba membahas pengamanan media penyimpanan portable, seperti flashdisk, hardisk eksternal, keping CD/DVD, SD CARD, memory stick, dll.

Sebagai media penyimpanan portable, tentunya sering dibawa kemana-mana, tidak tertutup kemungkinan bahwa media tersebut tidak sengaja jatuh ataupun dicuri orang. Bagi sebagian orang mungkin tidak terlalu berpengaruh dengan hilangnya media tersebut kareng hanya mengganti dengan media yang baru. Namun, bagaimana dengan data di dalamnya, bayangkan saja bila ada data yang menyangkut rahasia perusahaan besar dan sejenisnya, hal ini juga membahayakan untuk perusahaan tersebut, apalagi jatuh di tangan orang yang tidak bertanggung jawab. Oleh karena itulah, pada makalah ini, mencoba memberikan analisis terhadap teknologi pengamanan media penyimpanan portable untuk menjawab satu dari banyak tantangan peradaban yang ada.

## II. LANDASAN TEORI

### 2.1 **Dasar-dasar Penyimpanan File**

Sebuah file adalah koleksi informasi yang secara logic dikelompokkan menjadi sebuah entitas dan dipanggil (disebut) dengan nama yang unik, seperti filename. Untuk end user, biasanya ada dua tipe file: file data, seperti dokumen teks, spreadsheet, gambar, video, dll, dan file sistem, seperti sistem operasi, binary application, dan library-library. Suatu file sistem mendefinisikan cara bagaimana file-file yang ada diberi nama, disimpan, diorganisasi, dan diakses. Direktori, atau biasa dikenal dengan folder, adalah struktur organisasi yang digunakan oleh file sistem untuk mengelompokkan file. Fitur lain dari adalah metadata, "data tentang suatu data", dalam konteks file sistem, metadata adalah informasi mengenai file dan folder, seperti nama dari file atau folder, tanggal dibuat , dan ukuran.

File sistem dirancang untuk menyimpan folder, file sistem, file data, dan metadata dalam media penyimpanan digital. Namun, media penyimpanan (media penyimpanan di sini juga mencakup media penyimpanan portable) mungkin mempunyai data residu, yaitu data dari file yang dihapus (termasuk versi awal dari file-file yang ada dan file sementara/temporary). Data residu tersebut biasanya bisa dikembalikan (recovered) dari end user device lwat analisis forensik. Di bawah adalah bentuk-bentuk umum dari data residu:

- **Unused File Allocation Units**. File sistem menyimpan file dalam potongan-potongan yang disebut unit-unit alokasi file (file allocation unit). Unit-unit alokasi file adalah unit-unit dalam sebuah partisi yang berada dalam keadaan tidak sedang dipakai oleh file sistem. Ketika sebuah file dihapus, tidak serta-merta file tersebut dihapus secara fisik, tetapi informasi pada struktur data direktori yang menunjuk ke lokasi dari file tersebut ditandai "telah dihapus". Hal Ini berarti bahwa file tersebut masih disimpan dalam media tetapi tidak lagi dienumerasi oleh sistem operasi. Sistem operasi mengenali ini sebagai unused space/ ruang yang tidak dipakai dan bisa menimpa sebagian atau seluruh bagian dari file yang "telah dihapus" tersebut kapan saja.
- **Slack Space**. Meski suatu file membutuhkan ruang yang lebih kecil daripada ukuran unit alokasi file, keseluruhan dari unit alokasi tetap "reserved" untuk file yang akan dimasukkan ke media penyimpanan.Contohnya, jika alokasi unit file berukuran 32KB dan file yang akan dimasukkan berukuran hanya berukuran 7 KB, maka keseluruhan 32 KB tersebut akan dialokasikan untuk file dengan ukuran 7 KB tadi, hanya saja 7 KB yang digunakan, menghasilkan sisa ruang tak terpakai sebesar 25 KB. Ruang tak terpakai tersebut dinamakan file slack space, dan masih mungkin berisi data residu, sisa dari file yang "telah dihapus".
- **Free Space**. Free Space (ruang bebas/kosong) adalah area dalam media penyimpanan yang sedang tidak dialokasikan untuk sebuah partisi. Biasanya free space juga berupa ruang dalam media di mana terdapat file sisa, "telah dihapus". Free space mungkin berisi potongan-potongan data.

Sebelum media penyimpanan bisa digunakan untuk menyimpan file. Media tersebut terlebih dahulu dipartisi atau diformat menjadi volume logic (logical volumes). Proses partisi adalah aksi logic untuk membagi media menjadi bagian-bagian yang berfungsi sebgai unit yang terpisah. Suatu logical volume adalah partisi atau koleksi dari partisi-partisi yang berperan sebagai sebuah entitas tunggal yang telah diformat.dengan suatu file sistem. Beberapa tipe media hanya mampu mempuyai satu tipe partisi saja atau mungkin hanya satu logical volume saja, di saat yang lain mampu menampung banyak partisi.

### 2.2 **Media Penyimpanan Portable**

Secara umum, media penyimpanan portable bisa dibagi tiga, yaitu:

- *Data Storage Media* (media penyimpanan data). Termasuk di dalamnya bermacam-macam tipe dari kartu media, disk optik, dan magnetic tape – yang digunakan untuk menyimpan data dalam bentuk digital. Untuk terhubung dengan komputer ataupun sistem IT, media tipe ini membutuhkan interface berupa pembaca (reader, contohnya card reader untuk membaca SD Card, memory stick, memory card, dll) yang biasanya spesifik untuk tipe dan format tertentu dari media tersebut.
- Device dengan tambahan fungsi sebgai penyimpan data. Ini meliputi alat yang bisa digenggam, yaitu mobile device, seperti smartphones, PDA (personal digital assistant), kamera digital, PC tablet, gadget media player, dan semacamnya yang mempunyai kemampuan untuk menyimpan sejumlah data yang signifikan dalam bentuk digital selain kemampuan dasarnya. Hampir semua peralatanini bisa terhubung dengan sistem IT suatu enterprise lewat kabel atau peralatan nirkabel.
- *Data Storage Devices* (peralatan penyimpanan data). Peralatan yang dimaksud di sini adalah peralatan

yang dirancang dan didedikasikan secara spesifik untuk menyimpan data dalam bentuk digital. Yang termasuk dalan kategori ini adalah "thumb" drive atau flash drive, desktop travel drive, dan disk drive eksternal (yang menggunakan baik teknologi penyimpanan magnetik dan optik). Berbeda dengan storage media yang membutuhkan mekanisme reader, data storage device mampu terhubung secara langsung dengan komputer ataupun sistem IT lewat kabel dengan penghubung yang sesuai atau dalam beberapa kasus mampu dengan menggunakan koneksi nirkabel.

| Tipe Alat | Kapasitas Volume Data | Potensi Maksimum Tingkat Transfer Data |
|---|---|---|
| Optical Disk | 30 GB | 54 MB/s |
| Media Card | 32 GB | 45 MB/s |
| Magnetic Tape Cartridge | 5 TB | 80 MB/s |
| Media Player | 250 GB | 60 MB/s |
| "Thumb" Drive /Flash Drive | Up to 128 GB | 30 MB/s |
| Desktop Travel Drives | Up to 500 GB | 60 MB/s |
| External Hard Disk Drive | 2 TB | 3 Gb/s |

*Tabel 1Spesifikasi Media Penyimpanan Portable*

Berdasarkan tabel di atas atribut tersebut membuat media penyimpanan portable menjadi perangkat bisnis (dalam arti yang luas) yang cukup penting, misal saja untuk mendukung tenaga kerja dalam sebuah enterprise yang mobile dan bekerja dalam jarak yang jauh. Namun, atribut ini juga berarti sumber resiko dalam sebuah sistem IT di sebuah enterprise.

Pada makalah ini, analisis pengamanan akan lebih tertuju ke kategori yang pertama dan ketiga, yaitu data storage media data storage devices.

# III. ANALISISDAN TEKNOLOGI PENGAMANANAN

Pada makalah ini akan dijelaskan tentang teknologi pengamanan pada media penyimpanan portable pada saat ini, overview analisis resiko keamanan penggunaan media penyimpanan portable serta analisis terhadap teknologi yang digunakan untuk pengamananan tersebut.

## A. Analisis Resiko yang Timbul dari Adanya Sistem

Beberapa resiko yang ditimbulkan karena adanya media penyimpanan portable:

- Kehilangan dan pencurian perangkat.
Karena ukuran dari perangkat yang cukup kecil, akan sangat mudah perangkat untuk hilang atau dicuri orang, Jika data yang disimpan tidak dienkripsi, maka data akan sangat mudah diakses oleh siapa saja. Pada kasus perangkat seperti pada smartphone atau perangkat yang mempunyai fungsi tambahan sebagai media penyimpanan, perangkat tersebut akan juga mudah untuk dibongkar untuk mendapatkan akses terhadap komponen penyimpan data, sehingga mendapat akses terhadap data
- Pembuangan perangkat.
Ketika media penyimpanan portable dibuang, maka masih ada resiko data akan diakses oleh orang-orang yang tidak berhak seiring dengan data yang masih ada dalam perangkat. Data yang sudah dihapus secara manual dari perangkat mungkin masih ada secara fisik sampai data tersebut ditimpa oleh data yang baru. Terdapat beberapa software dan hardware yang mampu mengembalikan data-data tersebut, sehingga bisa diakses kembali.
- Pencurian data dari sistem IT.
Dengan adanya media penyimpanan portable mengindikasikan bahwa data sensitif dari personal maupun perusahaan bisa dicuri dari sistem IT dalam suatu enterprise. Ukuran perangkat yang kecil mampu membuat perangkat keluar masuk dari lingkungan enterprise tanpa menarik perhatian apalagi media penyimpanan pada media player tidak akan menarik perhatian sama sekali. Ketika sudah masuk lingkungan penyerang bisa terhubung dengan sistem lewat file sistem daripada lewat sistem jaringan mengakibatkan ancaman dari luar.
- Penolakan data.
Penyimpanan data pada media penyimpanan portable membawa resiko data yang bisa hilang karena kecelakaan atau aksi jahat penyerang. Di mana data disimpan dalam bentuk terenkripsi pada media penyimpanan portable, ada kemungkinan akan hilangnya atau lupa akan kunci untuk dekripsi data, sehingga tidak akan berguna bagi enterprise ataupun personal (data denial).
- Adanya malware.
Karena faktor portabilitas dari media, tentunya hal ini akan menjadi vektor bagi malware baik disengaja atau tidak disengaja.Orang yang melakukan eksploitasi malware tersebut mungkin menggunakan teknik-teknik social engineering utnuk memanipulasi pengguna untuk menghubungkan media penyimpanan portable yang sudah terinfeksi oleh malware untuk menyusupkannya ke komputer personal atau sistem IT dari sebuah enterprise.
- Adanya software atau data yang tidak diinginkan.
Sama halnya dengan malware, media penyimpanan portable bisa berperan sebagai perantara dan penyalur dari software ataupun data yang tidak diinginkan. Bisa juga berupa software hiburan yang tidak berpengaruh pada keamanan, tetapi akan mempengaruhi produktivitas dari individu dan enterprise.

B. **Teknologi Enkripsi pada Media Penyimpanan Portable**

Banyak teknologi yang sudah ada yang bisa dimanfaatkan untuk melakukan enkripsi data pada peralatan end user. Pada bagian ini akan dijelaskan teknologi yang umum dan biasa digunakan, proteksi yang disediakan dari tiap-tiap jenis teknologi, dan akan dijelaskan bagaimana melakukan manajemen dari tiap-tiap teknologi.

3.2.1 *Full Disk Encryption*

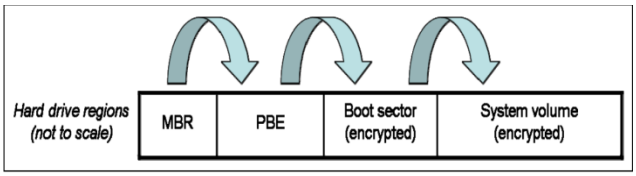
Full disk encryption (FDE), atau lebih dengan enkripsi disk penuh (whole disk encryption) adalah proses untuk melakukan enkripsi semua data dalam hard drive baik portable maupun non-portable yang digunakan untuk melakukan boot sebuah komputer, termasuk sistem operasi komputer, dan mengizinkan akses suatu data jika sukses melakukan autentifikasi produk yang menggunakan FDE. Kebanyakan produk dari FDE adalah software-based, jadi yang akan dibahas di sini adalah sofware-based FDE.

Software FDE bekerja dengan cara mengalihkan MBR (Master Boot Record) dari komputer, yang merupakan sektor yang reserved dalam media bootable yang nantinya akan menentukan software mana yang akan dieksekusi ketika komputer melakukan booting dari media. Sebelum software FDE diinstall dalam komputer, MBR biasanya akan menunjuk ke sistem operasi utama dari komputer.

3.2.2.1 Proses Enkripsi

Ketika software FDE sudah diinstall dan sedang digunakan, MBR komputer akan dialihkan ke lingkungan pra-boot khusus (pre-boot environtment/ PBE) yang mengontrol akses ke komputer. Pengalihan ini dapat dilihat pada gambar 1 di bawah.. PBE akan meminta user untuk melakukan autentifikasi dengan sukses, dengan memasukkan ID dan password, sebelum proses dekripsi dan melakukan booting sistem operasi. Proses ini dikenal dengan pre-boot authentication/PBA. Kebanyakan produk FDE mendukung baik autentifikasi berbasis jaringan maupun autentifikasi lokal untuk PBA.

Ketika PBA sukses dilakukan, software FDE akan melakukan dekripsi boot sector dari sistem operasi, seperti pada gambar 1, dan boot loader dalam boot sector akan melakukan load sistem operasi. Saat me-load, software FDE melakukan dekripsi file-file sistem operasi (yang disimpan dalam volume sistem) yang dibutuhkan, yang dapat dilihat di gambar 1 di bawah. Saat sistem operasi selesai melakukan booting, pengguna melakukan autentifikasi sistem operasi dan menggunakan komputer seperti biasa. Ketika pengguna perlu untuk membuka file yang terenkripsi, menyimpan file baru, atau melakukan operasi lain yang berhubungan dengan hard drive, software FDE secara transparan melakukan dekripsi dan enkripsi sektor dari harid drive yang dibutuhkan saja. Hal ini mungkin secara marginal dapat meningkatkan waktu yang dibutuhkan untuk membuka atau menyimpan file dari biasanya, tetapi waktu tunda umumnya bisa diperhatikan ketika sedang melakukan operasi pada file yang berukuran besardan banyak. Pada komputer yang terproteksi dengan FDE, pengguna dapat memperhatikan waktu tunda untuk beberapa detik ketika melakukan booting atau mematikan komputer. Waktu tunda juga ada ketika sedang menjalankan fitur "hibernate", karena software FDE harus melakukan enkripsi dan dekripsi file hibernasi yang cukup besar (yang termasuk penggandaan dari memori komputer) yang disimpan dalam hard drive. Lamanya waktu tundat bergantung pada ukuran dari memori, ukuran hard drive, kecepatan dan faktor lain.




*Gambar 1 Urutan Booting untuk Software Full Disk Encryption*

3.2.2.2 Analisis

Karena FDE mengubah prosedur booting komputer, hal tersebut dapat menyebabkan masalah operasional. Misalnya, melakukan modifikasi MBR dapat mencegah komputer dengan konfigurasi dual-boot untuk berfungsi sebagaimana mestinya, dan menyimpan PBE di ruang di antara MBR dan boot sector dapat menyebabkan konflik dengan software lain, seperti software peralatan-peralatan disk-level, yang juga menaruh kodenya di ruang tersebut. Device yang terproteksi dengan FDE mungkin juga mengalami masalah dengan peralatan manajemen aset dan penggunaan LAN.

Software FDE secara umum digunakan dalam komputer dan laptop. Persyaratan untuk PBA berarti pengguna harus mampu melakukan autentifikasi dengan komponen yang paling fundamental dari sebuah device, seperti keybiard standard, karena sistem operasi belum diload, driver untuk level sistem operasi tidak ada. Contohnya, sebuah PDA atau smartphone tidak bisa menampilkan on-screen keyboard, karena hal tersebut kemampuan yang dimiliki di tingkat sistem operasi.

FDE bisa juga dibuat dalam bentuk sebuah hard drive disk controller. FDE berbasis software dan hardware memberikan kemampuan yang mirip dengan mekanisme yang berbeda. Ketika pengguna mencoba untuk melakukan booting device yang terproteksi dengan FDE berbasis hardware, hard drive akan meminta pengguna untuk melakukan autentifikasi sebelum melakukan load sistem operasi. Kemampuan FDE untuk dibuat dalam bentuk perangkat keras dalam suatu cara tidak bisa dinonaktifkan maupun dilepas dari drive. Kode enkripsi dan yang melakukan autentifikasi, seperti password dan kunci kriptografi, disimpan dengan aman dalam hard drive. Karena proses dekripsi dan enkripsi dilakukan oleh hard drive, tanpa partisipasi sistem operasi, alhasil ada dampak terhadap performa meskipun sangatlah kecil.

Perbedaan mencolok antara FDE berbasis software dan

hardware adalah FDE berbasis software dapat diatur secara terpusat, tetapi FDE berbasis hardware hanya mampu diatur dalam area lokal saja. Hal ini membuat manajemen kunci dan aksi/proses recovery pada FDE berbasis hardware biasanya lebih banyak memakan resource secara intensif dan tidak praktis daripada FDE berbasis software. Perbedaan lain yang mencolok adalah karena FDE berbasis hardware melakukan semua pemrosesan kriptografi dalam hard drive dari hardware, maka tidak perlu meletakkan kunci kriptografi dalam memori komputer, sehingga cukup potensial untuk malware dan ancaman-ancaman lain dalam mendapatkan kunci tersebut. Perbedaan ketiga yang cukup signifikan adalah FDE berbasis hardware tidak mengubah MBR, sehingga FDE berbasis hardware tidak mennimbulkan konflik dengan software yang melakukan modifikasi pada MBR (misalnya konfigurasi dual-boot).

3.2.2 *Virtual Disk Encryption dan Volume Encryption*

Virtual disk encryption adalah proses untuk melakukan enkripsi sebuah file yang disebut container/penampung, yang mampu menampung banyak file dan folder, dan mengijinkan untuk mengakses data dalam penampung setelah autentifikasi yang sesuai, penampung biasanya dimount sebagai disk virtual. VDE digunakan di segala jenis perangkat penyimpanan. Penampung adalah file tunggal yang berada dalam sebuah volume logic. Contoh dari volume adalah boot, sistem, data dari volume dalam sebuah PC, dan sebuah USB flas drive yang diformat dengan sebuah file sistem. Volume encryption atau enkripsi volume adalah proses untuk melakukan enkripsi seluruh volume logic dan mengijinkan akses data ke terhadap hanya setelah melakukan autentifikasi yang disediakan. Enkripsi volume sering dilakukan pada data volume pada hard drive dan media penyimpanan portable berbasis volume, seperti USB flash drive dan hard drive externa;. Enkripsi volume dari boot dan volume sistem adalah bentuk khusus dari FDE yang sangat penting.

3.2.2.1 Proses

Pada level yang cukup tinggi, VDE dan enkripsi dilakukan dengan sama. Software berjalan pada sistem operasi yang digunakan untuk mengakses volume dan penampung menangani semua proses untuk read dan write dari volume atau penampung yang diproteksi. Ketika sistem operasi berhasil di load, jika pengguna ingin menggunakan volume atau penampung yang dienkripsi, volume dan penampung akan dimount setelah pengguna mengisikan atau memberikan autentifikasi yang diperlukan. Setelah itu, software akan secara otomatis melakukan dekripsi dan enkripsi sektor yang sesuai dan diperlukan. Hal ini mengakibatkan pertambahan waktu untuk membuka atau menyimpan file, tetapi waktu tunda dapat diperhatikan saat beroperasi dalam file berukuran besar. Waktu tunda juga terjadi saat melakukan mount dan unmount dari volume dan penampung yang dienkripsi.

3.2.2.2 Analisis

Perbedaan utama antara enkripsi volume dan VDE adalah penampun atau container lebih portable dan volume tidak, penampung dapat digandakan dari satu medium ke medium yang lain, dengan enkripsi yang masih melekat. Hal ini memungkinkan, penampung untuk diburn dalam CD ataupun DVD dan bisa digunakan dalam media lain yang bukan berbasis volume. VDE juga membuat back up data yang penting menjadi sangat mudah; penampung hanya cukup menyalin ke server atau media backup. Keunggulan lain dari VDE adalah dibanding enkripsi volume adalah VDE bisa digunakan pada situasi di mana media removable berbasis volume perlu untuk mempunyai baik bagian penyimpanan yang terproteksi maupun yang tidak terproteksi dengan cara volume dibiarkan tidak terproteksi dan penampung diletakkan dalam volume untuk informasi-informasi serta data yang sensitif maupun penting.

Beberapa produk VDE, lebih jauh juga mendukung mobilitas dengan memberikan fitur yang bisa meletakkan file-file executable dalam media yang terdapat penampung di dalamnya, dengan metode seperti menginstall driver pada komputer atau menjalankan autentifikasi dan utility untuk melakukan dekripsi.Konten yang diproteksi dalam media bisa diakses oleh pengguna setelah pengguna terlebih melakukan autentifikasi yang diminta dengan sukses.

Beban dari pengguna untuk CDE dan enkripsi volume berbeda-berbeda, utamanyabergantung pada akses kontrol dari device. Contohnya, jika sistem operasi dari laptop dikonfigurasi sehingga pengguna hanya mampu melakukan write file saja ke penampung atau volume yang dienkripsi, jadi pengguna tidak perlu repot-repot memastikan bahwa file disimpan pada lokasi yang sesuai. Namun, jika sistem operasi tidak dikonfigurasi seperti ini, mengijinkan pengguna untuk menyimpan file pada lokasi yang berbeda-beda, atau jika device yang dienkripsi adalah media removable yang tidak diproteksi lewat fitur akses kontrol, maka pengguna akan dibebani untuk memastikan bahwa mereka menyimpan file pada lokasi yang sesuai, Pada kasus ini, jika pengguna gagal melalui prosedur yang diperlukan, maka beberapa file yang harusnya diproteksi maka tidak akan terproteksi.

3.2.3*File/Folder Encryption*

Enkripsi file adalah proses untuk melakukan enkripsi file tersendiri (yang diinginkan saja) pada media penyimpanan dan mengijinkan akses ke data yang terenkripsi jika telah melakukan autentifikasi yang dimint. Enkripsi folder mirip dengan enkripsi file, hanya saja enkripsi dilakukan pada folder-folder tersendiri bukan pada file. Beberapa sistem operasi menyediakan enkripsi folder maupun file sebagai fitur di dalamnya, dan banyak program dari pihak ketiga yang sudah ada dan bisa dipakai.

3.2.3.1 Proses

Meskipun enkripsi folder dan VDE terlihat mirip, baik

folder dan penampung dimaksudkan untuk menampung dan memproteksi beberapa file, tetapi terdapat perbedaan dalam dua metode tersebut. Sebuah penampung adalah sebuah file tunggal (opaque file) yang artinya tidak ada orang yang mampu melihat folder atau file yang berada di dalam penampung tersebut sampai penampung tersebut didekripsi. Enkripsi folder dan file transparan (bukan opaque), berarti siapa saja dengan akses terhadap file sistem bisa melihat nama dan metadata lain dari file dan folder yang dienkripsi, termasuk file dan folder di dalam folder yang terenkripsi, jika file dan folder tersebut tidak diproteksi oleh sistem operasi dengan fitur akses kontrol. Enkripsi file dan folder bisa digunakan dalam semua tipe media penyimpanan. Opsi yang biasanya ada:

- membiarkan user untuk memilih file dan folder yang ingin dienkripsi
- melakukan enkripsi konten yang ditunjuk oleh administrator dengan otomatis
- melakukan enkripsi file-file tertentu, file dengan ekstensi tertentu secara otomatis
- melakukan enkripsi semua file yang ditulis (write) oleh aplikasi tertentu secara otomatis
- melakukan enkripsi semua file data untuk pengguna tertentu secara otomatis

3.2.3.2 Analisis

Enkripsi file dan folder bisa diemplementasikan dalam banyak cara, lewat driver, service, dan aplikasi. Ketika pengguna mencoba untuk membuka file terenkripsi (baik file itu yang dienkripsi atau folder tempat file tersebut yang dienkripsi), software akan meminta pengguna untuk melakukan autentifikasi dengan sukses. Setelah autentifikasi dilakukan, software akan melakukan dekripsi secara otomatis file yang dipilih untuk dibuka. Karena mekanisme dilakukan dengan cara dekripsi satu file dalam satu waktu. Kinerja dari enkripsi file ataupun folder bisa diminimalisasi. Enkripsi file dan folder umumnya sering digunakan untuk enkripsi file data, seperti dokumen (word documents) dan spreadsheet. Solusi yang berupa enkripsi file dan folder terkadang mampu melakukan enkripsi pada swap file, tetapi untuk file yang biasanya bukan berupa file untuk hibernasi dan file executable dari sistem operasi.

Banyak produk enkripsi file dan folder memberikan pilihan untuk memilih file dan folder yang akan dienkripsi dan mengikutsertakan pengguna dalam prosesnya, dengan enkripsi secara manual untuk tiap file dan folder baru membutuhkan proteksi, mengingat-ingat di mana lokasi tempat file dan folder disimpan, atau malah tidak melakukan apapun karena file dan folder dienkripsi dengan otomatis.

Banyak juga aplikasi, seperti aplikasi untuk kompresi dan aplikasi untuk produktivitas kantor yang memberkan kemampuan untuk enkripsi file dan folder, tetapi terbatas. Aplikasi tersebut bergantung secara penuh pada pengguna untuk memastikan bahwa file yang diinginkan benar-benar terenkripsi. Aplikasi macam ini sering tidak diatur terpusat, yang membuat manajemen kunci aspek lain dari manajemen dari penggunaan fitur dari aplikasi enkripsi file dan folder menjadi lebih rumit.

### C. **Proteksi yang Diberikan oleh Teknologi Enkripsi pada Media Penyimpanan Portable**

3.3.1 *Full Disk Encryption*

Untuk komputer yang sedang tidak melakukan boot, semua informasi yang dienkripsi dengan FDE terproteksi, dengan asumsi dibutuhkan PBA. Ketika komputer sudah di boot, asumsi sudah dilakukan autentifikasi, FDE tidak akan memberikan proteksi, dan setelah sistem operasi di load, sistem operasi bertanggung jawab penuh atas proteksi informasi yang tidak dienkripsi. Terdapat pengecualian bila komputer/device berada dalam keadaan sedang hibernasi, kebanyakan produk FDE mampu melakukan enkripsi file hibernasi.

3.3.2 *Virtual Disk and Volume Encryption*

Ketika VDE digunakan, konten dari penampung diproteksi sampai pengguna melakukan autentifikasi pada penampung tersebut. Jika dalam prosedurnya digunakan single-sign on, berarti penampung yang ada diproteksi sampai pengguna menggunakan perangkat dengan memasukkan single-sign on. Jika single-sign on tidak digunakan, maka proteksi dilakukan sampai pengguna melakukan autentifikasi secara eksplisit. VDE tidak menyediakan untuk data di luar penampung, termasuk swap file dan file hibernasi yang mungkin berisi file yang tidak dienkripsi dan masih berada dalam memori. Enkripsi volume memberikan proteksi yang sama seperti VDE, hanya saja dalam bentuk volume bukan penampung.

3.3.3 *File/Folder Encryption*

Enkripsi file dan folder melakukan proteksi konten atas file yang dienkripsi (termasuk file di dalam folder yang dienkripsi) sampai pengguna melakukan autentifikasi untuk file dan folder tersebut. Enkripsi file dan folder tidak memberikan proteksi di luar file dan folder yang diproteksi, , termasuk swap file dan file hibernasi yang mungkin berisi file yang tidak dienkripsi dan masih berada dalam memori. Software enkripsi file dan folder juga tidak bisa memberikan proteksi untuk menjaga kerahasiaan dari nama file dan metadata lain, yang mungkin bisa memberikan informasi bagi penyerang (contohnya file yang diberi nama dengan nomor KTP atau tanggal lahir).

## IV. ANALISIS ANCAMAN, SOLUSI KEAMANAN TERHADAP ANCAMAN, SERTA PERBANDINGAN TEKNOLOGI MEDIA PENYIMPANAN PORTABLE

A.**Analisis Umum tentang Teknologi Enkripsi Media Penyimpanan Portable, Kemungkinan terhadap Serangan yang AdabesertaUsulan Solusinya (penanganan untuk ancaman keamanan pada tiap teknologi)**

Pada banyak kasus, khususnya untuk FDE dan enkripsi volume, produk-produk yang ada tidak memberikan proteksiuntuk file yang disalin atau dipindahkan dari media yang terenkripsi ke lokasi lain (lokal atau jaringan lain), karena produk tersebut akan melakukan dekripsi seiiring dengan bagian dari file disalin atau dipindahkan. Lokasi tujuan bertanggung jawab atas proteksi file, dan tidak ada proteksi yng dapat diberikan saat transit dari sumber ke tujuan. Namun, beberapa teknologi enkripsi memungkinkan proteksi untuk diberikan jika pengguna menginginkan. Hampir semua produk VDE memungkinkan sebuah penampung (secara keseluruhan) untuk dipindahkan, termasuk proteksi terhadap penampung tersebut, tetapi file dan folder yang dipindahkan dari penampung tersebut tidak akan diproteksi. Beberapa produk enkripsi file dan folder mampu mempertahankan proteksinya walaupun file atau folder sedang disalin atau dipindahkan, pada beberapa kasus ini bisa dilakukan dalam satu file sistem, dan pada kasus yang lain bisa dilakukan dari satu file sistem ke file sistem yang lain.

Ancaman utama untuk semua tipe teknologi yang dijelaskan adalah akses informasi ilegal dan tidak sah pada peralatan atau media yang hilang atau dicuri. VDE, enkripsi volume, enkripsi file, dan folder bisa mengurangi ancaman pada level aplikasi dan sistem operasi terhadap informasi yang diproteksi, termasuk malware, remote access, dan metode-metode lain yang bergantung saat OS sedang booting, sampai pengguna sukses malakukan autentifikasi. Ketika autentifikasi terjadi, maka segala macam proses yang sedang dijalankan pada perangkat tersebut (seperti malware) dengan akses terhadap file pengguna bisa mendapatkan informasi yang didekripsi. Karena file hanya diproteksi sampai saat autentifikasi sukses dilakukan, akan lebih berguna bilakita menggunakan solusi keamanan yang dikonfigurasikan hanya untuk melakukan dekripsi pada file yang diperlukan (lebih baik melakukan enkripsi file atau folder pada 10 file yang sensitif daripada melakukan enkripsi volume untuk mengenkripsi 10 file sensitif ditambah 1000 file yang tidak sensitif). Lebih banyak file yang diproteksi, maka pengguna akan lebih cepat dan lebih sering melakukan autentifikasi terhadap media penyimpanan yang akan meningkatkan tingkat exposure file yang didekripsi.

Beberapa produk juga mengijinkan enkripsi untuk satu atau beberapa pengguna dalam sebuah perangkat. Jika terdapat enkripsi untuk satu pengguna, kerahasiaan media penyimpanannya terproteksi dari pengguna lain (termasuk juga administrator) yang menggunakan perangkat yang sama. Enkripsi untuk beberapa pengguna memungkinkanuntuk sharing data-data sensitif antar pengguna yang berhubungan dan berhak, dan di saat sama juga melakukan proteksi terhadap pengguna lain yang tidak berkepentingan. Mekanisme ini memberikan proteksi terhadap ancaman dari dalam.

Pada beberapa kasus, beberapa tipe teknologi bisa digunakan bersama-sama untuk memberikan proteksi terhadap tipe-tipe ancaman yang berbeda-beda, misalnya FDE bisa digunakan untuk melakukan proteksi semua data pada perangkat saat perangkat hilang atau dicuri, dan enkripsi file, folder, dan volume bisa digunakan untuk memberikan proteksi tambahan atas beberapa data yang sensitif dan data lainnya.

Ketika berbicara tentang ancaman, organisasi atau individu harus menyadari bahwa setelah teknologi pengamanan sudah diimplementasikan, mungkin ada beberapa sisa data pada perangkat yang tertinggal dan tetap tidak terproteksi, Contohnya, ketika sebuah file dienkripsi menggunakan enkripsi file atau folder dan file aslinya dihapus, sisa dari plainteks asli dari file mungkin masih ada pada media penyimpanan. Contoh lain adalah produk FDE dan enkripsi volume yang hanya melakukan enkripsi pada sektor disk yang berisi file yang diinginkan, bukan sektor disk yang hanya berisi file yang sudah dihapus dan sisa-sisa data. Sisa-sisa ini mungkin dikembalikan dengan alat forensik oleh penyerang yang mendapatkan akses fisik ke komputer, tanpa harus memberikan autentifikasi apapun. Organisasi dan personal harus menyadari ancaman terhadap baik file maupun sisa-sisa dari file.

Organisasi harus menyadari bahwa jika perangkat pengguna dikompromikan setiap saat, setiap teknologi enkripsi penyimpanan pada perangkatnya mungkin tidak efektif untuk sebagian atau keseluruhan perangkat. Sebagai contoh, bila perangkat sedang digunakan dan pengguna telah melakukan autentifikasi, malware dapat mengakses file yang didekripsi dan mentransfer salinan file ke host eksternal atau mengekstrak informasi sensitif dari file tersebut. Contoh lain adalah penyerang menonaktifkan atau melakukan konfigurasi ulang enkripsi penyimpanan, atau malware memasang keylogger untuk mendapatkan password yang digunakan untuk autentifikasi enkripsi penyimpanan, atau malware mengakuisisi salinan dari kunci enkripsi penyimpanan dari memori perangkat (untuk enkripsi penyimpanan berbasis software).

Organisasi juga harus menyadari bahwa mereka tidak harus bergantung pada teknologi enkripsi penyimpanan untuk proteksi data tanpa harus secara teratur mempertahankan solusi enkripsi. Sebagai contoh, jika seorang penyerang memperoleh device yang hilang, dicuri, atau sudah aus diproteksi oleh teknologi enkripsi penyimpanan, dan kerentanan dalam teknologi enkripsi untuk media penyimpananditemukan di masa depan, penyerang mungkin dapat memanfaatkan untuk mengaksesdata yang diproteksi.

B.**Perbandingan dan Pemilihan Teknologi Enkripsi**

Di bawah dapat dilihat tabel perbandingan antar teknologi enkripsi yang ada pada masa sekarang.

| Karakteristik | Full Disk Encryption | Volume Encryption | Virtual Disk Encryption | File and Folder Encryption |
|---|---|---|---|---|
| Platform yang didukung | Komputer desktop dan laptop | Komputer desktop , laptop, dan removable media berbasis volume (seperti USB flash drive) | Semua jenis perangkat | Semua jenis perangkat |
| Data yang diproteksi oleh enkripsi | Semua data pada media (file data, file sistem, file sisa, dan metadata) | Semua data pada volume (file data, file sistem, file sisa, dan metadata) | Semua data pada penampung (file data, file sisa, dan metadata, tapi tidak termasuk file sistem) | File dan folder yang dipilih saja (hanya file data) |
| Mengurangi resiko ancaman yang disebabkan oleh perangkat yang hilang atau dicuri | Ya | Ya | Ya | Ya |
| Mengurangi ancaman di tingkat sistem operasi dan aplikasi (seperti malwaredan ancaman dari dalam) | Tidak | Jika data pada volume diproteksi, terkadang akan mengurangi ancaman-ancaman tersebut. Jika volume tidak sedang diproteksi, maka tidak akan ada antisipasi terhadap ancaman tersebut | Terkadang melakukan antisipasi terhadap ancaman-ancaman tersebut | Terkadang melakukan antisipasi terhadap ancaman-ancaman tersebut |
| Berpotensi untuk memberi dampak pada perangkat bila terdapat kegagalan pada solusi enkripsi | Hilangnya seluruh data dan fungsionalitas perangkat | Hilangnya seluruh data pada volume yang berpengaruh pada fungsionalitas perangkat, tergantung pada volume mana yang sedang diproteksi | Hilangnya seluruh data pada penampung | Hilangnya seluruh data pada file dan folder yang dienkripsi |
| Portabilitas dari informasi yang dienkripsi | Tidak portable | Tidak portable | Portable | Portable |

*Tabel 2 Perbandingan Teknologi Enkripsi pada Saat Ini*

Ketika memilih teknologi untuk enkripsi pada media penyimpanan portable, beberapa hal harus diperhatikan untuk menentukan teknologi mana, membutuhkan infrastruktur serta perangkat apa yang harus diubah. Sebagai contoh, dengan menggunakan beberapa teknologi akan membutuhkan server dan software tambahan pada perangkat, di mana teknologi tidak membutuhkan hal-hal semacam itu.

### C. **Analisis Pemakaian Algoritma Enkripsi pada Teknologi Pengamanan dan Enkripsi Media Penyimpanan Portable**

Untuk algoritma enkripsi, pada makalah ini tidak akan dibahas secara spesifik tentang algoritma yang dipakai dalam proses enkripsi pada teknologi-teknologi yang disebutkan di atas. Menurut hasil analisis pada studi literatur yang ada ,pengaruh terbesar pada pengamanan dan enkripsi bukan berasal dari algoritma enkripsi yang nantinya akan dipakai, tetapi lebih kepada teknologi enkripsi yang akan dipakai.

Memang algoritma enkripsi juga berpengaruh dalam keamanan, tetapi selama ini kebanyakan kasus untuk serangan-serangan yang ada bukan pada memecahkan kunci atau algoritma dekripsi, melainkan berfokus pada memanfaatkan celah-celah yang ada pada teknologi enkripsi media penyimpanan dan memanfaatkan kelengahan user lewat teknik social engineering. Karena notabene hasilnya lebih cepat daripada harus melakukan pemecahan kunci dan algoritma yang dipakai.

Untuk algoritma yang sering dipakai adalah AES (*Advanced Encryption Standard*), standard enkripsi kunci simetri yang sudah banyak dipakai di seluruh dunia. Untuk mengatasi kelemahan dan kelengahan yang ada pada sisi pengguna, penulis *mengusulkan*manajemen kunci yang baik, keamanan juga bisa dijamin pada teknologi enkripsi media penyimpanan portable.

## V. KESIMPULAN

Dari hasil analisis di atas dapat diambil beberapa kesimpulan, yaitu:

- adanya teknologi penyimpanan media portable membawa ancaman dan resiko bagi kehidupan baik dalam personal maupun dalam enterprise
- ada tiga macam teknologi yang ada untuk saat ini untuk melakukan pengamanan dan enkripsi pada media penyimpanan
- tiap teknologi mempunyai kelebihan dan kelemahan tersendiri dalam mekanisme pengamanannya
- kombinasi beberapa teknologi enkripsi pada media penyimpanan portable dapat meningkatkan keamanannya
- untuk saat tidak ada teknologi yang 100% persen mampu memberi keamanan maksimal pada media penyimpanan portable
- banyak hal yang perlu dipertimbangkan ketikan akan mengimplementasikan teknologi enkripsi pada media penyimpanan portable, karena tiap teknologi membawa resiko tersendiri
- manajemen kunci yang baik akan cukup membantu dalam menjamin keamanan pada media penyimpanan portable
- pengaruh terbesar pada pengamanan dan enkripsi media penyimpanan portable bukan berasal dari algoritma enkripsi, melainkan pada implementasi teknologi yang dipakai

## REFERENSI


[1] Munir, Rinaldi, , slide kuliah IF3058 *Advanced Encryption Standard*, hal. 1-33.

[2] Munir, Rinaldi, , slide kuliah IF3058 Kriptografi pada Kehidupan Sehari-hari, hal. 1-28.

[3] http://csrc.nist.gov/publications/nistpubs/ diakses pada Sabtu, 7 Mei 2011

[4] http://daf.csulb.edu/offices/vp/information_security/policies/elec_data_security_portable_devices.htm diakses pada Minggu, 24 April 2011

[5] http://en.wikipedia.org/wiki/Advanced_Encryption_Standard Minggu, 8 Mei 2011

[6] http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_softwarediakses pada Minggu, 24 April 2011

[7] http://en.wikipedia.org/wiki/Data_remanence diakses pada Minggu, 24 April 2011.

[8] http://en.wikipedia.org/wiki/Secure_USB_Drivediakses pada Minggu, 24 April 2011

[9] http://en.wikipedia.org/wiki/USB_flash_drivediakses pada Minggu, 24 April 2011

[10] http://it.toolbox.com/blogs/adventuresinsecurity/portable-storage-device-security-8995 Sabtu, 7 Mei 2011

[11] http://www.cososys.com/white_papers/White_Paper_Biometric_Portable_Data_Protection_CoSoSys.pdf Sabtu, 7 Mei 2011

[12] http://www.ied.edu.hk/its/policies/portablestorage.htmldiakses pada Minggu, 24 April 2011

[13] http://www.spamlaws.com/portable-devices-security.html Sabtu, 7 Mei 2011

[14] http://www.tisn.gov.au/www/tisn/rwpattach.nsf/VAP/(C7C220BBE2D77410637AB17935C2BD2E)~PDSDSecurity-CIOPaper.pdf/$file/PDSDSecurity-CIOPaper.pdf Sabtu, 7 Mei 2011

[15] http://www.truecrypt.org/ diakses pada Minggu, 24 April 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, 9 Mei 2011

ttd

Aridarsyah Eka Putra
13507058