PENDAHULUAN

1.1 Latar belakang

Seiring dengan perkembangan teknologi, maka diikuti pula sarana penting yang mendukungnya, yaitu perangkat lunak serta perangkat keras komputer. Bersamaan dengan itu semakin banyak bermunculan para cracker yang dengan mudah merusak serta mengubah system keamanan dari suatu software. Hal ini tentu sangat tidak menyenangkan serta melanggar Hak Intelektual pembuat software tersebut. Sehingga meyebabkan kerugian baik secara materiil maupun secara intelektual.

Perkembangan seperti ini sangatlah merugikan banyak pihak, sehingga dibutuhkan suatu sistem keamanan yang dapat mengatasinya. Sistem keamanan yang dibutuhkan adalah sistem keamanan yang dapat memproteksi suatu software dari penggandaan serta pengubahan tanpa sepengetahuan maupun seizin pemiliknya atau pemegang lisensi.

Software proteksi ini nantinya dengan menyisipkan sebuah kode disebut STUB yang didalamnya terdapat nomor seri USB drive sebagai kunci proteksinya. Untuk menghindari membengkaknya ukuran file yang di proteksi maka nantinya juga akan di kompres sehingga memiliki ukuran yang tidak lebih besar dari ukuran file sebenarnya serta akan di lakukan proses enkripsi untuk bisa lebih mengamankan file aplikasi proteksi. Software ini tidak dapat diakses atau dijalankan jika USB yang merupakan kuncinya tidak terhubung pada PC dimana software tersebut akan dijalankan.

1.2 Perumusan masalah

Permasalahan yang dijadikan objek penelitian dan pengembangan pada tugas akhir ini adalah bagaimana kita mengamankan software berupa file executable (*.exe) yang akan dibungkus oleh aplikasi proteksi sehingga cracker ataupun hacker tidak dapat merubah atau menjalankannya. Selain itu aplikasi proteksi software ini juga diharapkan tahan terhadap serangan berupa: debugging, copying, breakpoint serta perubahan data binary dari pihak-pihak yang tidak berkepentingan.

Batasan masalah dalam tugas akhir ini adalah :

1. Komputer yang akan digunakan untuk memproteksi harus memiliki USB port.
2. Asumsi driver USB yang digunakan sebagai proteksi sudah terinstal.
3. Aplikasi hanya dapat memproteksi dari beberapa hacking tool, yaitu :
   - Regmon.
   - Filemon.
   - W32Dasm.
   - OllyDB.

4. File aplikasi yang bisa di proteksi merupakan file PE standar. Belum di *compress* atau di *encrypt* oleh software proteksi lainnya.

1.3 Tujuan

Adapun tujuan dalam tugas akhir ini adalah membangun sebuah sistem yang mampu :

1. Membuat suatu kode STUB yang mengambil nomor serial dari USB Storage untuk digunakan sebagai otentikasi atau validasi sistem proteksi.
2. Membuat sistem pengaman software dengan menyisipkan kode STUB ke dalam file aplikasi yang akan di proteksi serta melakukan proses kompresi dan enkripsi terhadap file aplikasi tersebut.
3. Mengamankan file aplikasi atau software tanpa merusak informasi yang ada pada software tersebut.
4. Melakukan pengujian kemampuan sistem proteksi menghadapi beberapa software yang digunakan sebagai cracking software seperti OllyDBG, RegMon, FileMon dan WinDASM32.

1.4 Metodologi penyelesaian masalah

Metode pemecahan masalah yang digunakan dalam pembuatan tugas akhir ini adalah :

- Studi literatur
  Mempelajari dasar teori mengenai proteksi, hacking, cracking suatu software.
- Analisis dan perancangan perangkat lunak
  Membuat analisis dan perancangan perangkat lunak dengan menggunakan analisa dan perancangan berbasis objek oriented.
- Implementasi perancangan perangkat lunak
  Mengimplementasikan perancangan perangkat lunak dalam Aplikasi Software proteksi menggunakan Serial number USB Drive sebagai kuncinya.
- Uji coba dan evaluasi sistem
  Menguji perangkat lunak yang telah dibuat untuk mengukur tingkat performansi dan keamananyanya, kemudian akan dilakukan analisis dan evaluasi dari hasil uji coba ini.
- Penyusunan Laporan Tugas Akhir.