Steganopassword sebagai Validasi Login User

Adrian Edbert Luman - 13507057
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]author@itb.ac.id

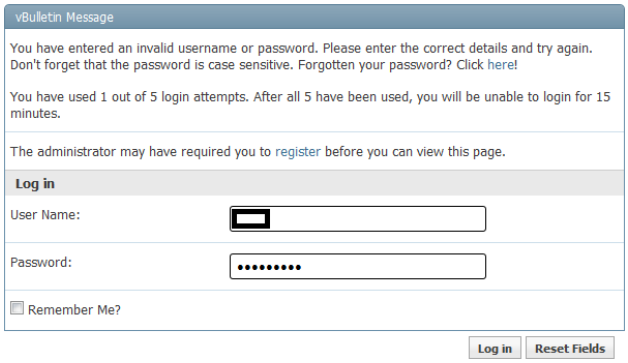
Abstrak – Makalah ini coba membantu memecahkan permasalahan banyaknya kasus kehilangan informasi berharga akibat serangan hacker. Validasi login ke dalam suatu situs atau suatu basis data sekarang ini menggunakan dua buah data bertipe string yang biasa disebut sebagai username dan password. Metode ini terbukti sangat sulit untuk dipecahkan dengan menggunakan beberapa metode penyerangan untuk validasi login ini. Namun ada beberapa metode yang dapat dengan mudah menembus keamanan ini, contohnya dengan menggunakan sniffer atau keylogger. Kedua cara ini bekerja tidak dengan cara melakukan penyerangan terhadap username dan password, namun lebih ke cara yang terkesan primitif. Keduanya mencoba mencuri isi dari username dan password pada saat diketikkan atau dikirmkan. Penggunaan steganografi sebagai validasi login adalah cara baru yang diharapkan dapat mengatasi kelemahan validasi dari kedua tipe serangan ini.

Kata Kunci : Key Logger, Sniffer, Steganografi, Validasi Login

I. PENDAHULUAN

Dewasa ini ada banyak sekali hal yang membutuhkan validasi login. Selain berbagai situs jejaring sosial seperti : Facebook, Friendster, Twitter; validasi login juga melindungi berbagai hal penting yang berkaitan dengan informasi penting seperti : basis data, dokumen Google; dan hampir semuanya menggunakan metode yang sama, yaitu penggunaan username dan password sebagai identifikasi user.

Hal ini menimbulkan pertanyaan mengenai seberapa tinggi tingkat keamanan metode tersebut. Faktanya metode ini terbukti cukup aman, kombinasi dua buah string serta banyaknya user yang terdaftar menjadikan sangat sulit untuk menemukan dengan tepat rangkaian username dan password yang sesuai dengan user yang menjadi target serangan. Belum lagi ditambah dengan berbagai metode tambahan untuk melindungi user, seperti dengan cara membatasi jumlah percobaan login untuk melindungi user dari serangan secara *brute-force* (Facebook, Indowebster) atau dengan membuat segel sign-in (Yahoo, Facebook).



Namun tetap saja segala keamanan itu tidak berarti seandainya informasi username dan password berhasil didapatkan oleh para hacker. Ada banyak cara yang bisa dilakukan oleh seorang hacker untuk meretas informasi username dan password yang dimiliki. Contoh paling mudah adalah dengan aplikasi sniffer atau keylogger.

Dengan menggunakan aplikasi sniffer atau keylogger ini hacker bisa mendapat informasi username dan

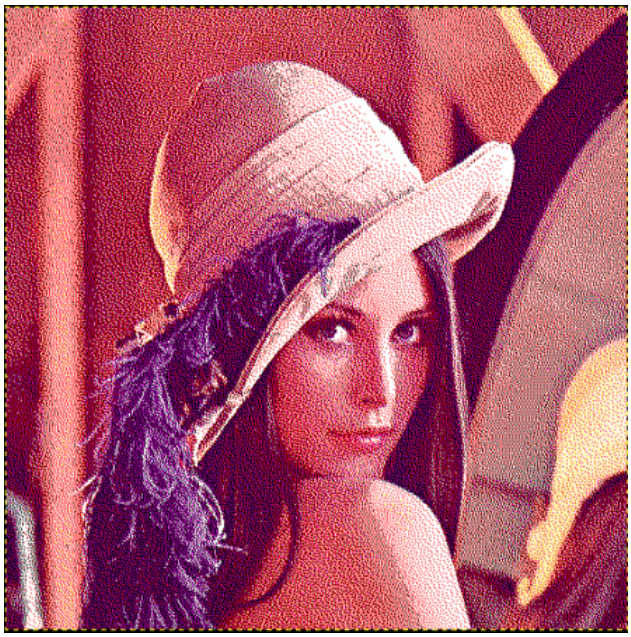
password tanpa harus melakukan metode-metode penyerangan yang rumit ataupun menghabiskan banyak waktu mencoba menyerang dengan brute-force. Hal ini karena kedua cara tersebut menggunakan metode primitif, yaitu dengan cara mengambil informasi username dan password yang diinginkan dari user itu sendiri.

Penggunaan sniffer dan keylogger sendiri merupakan masalah yang timbul dari sharing. Baik itu sharing unit komputer ataupun sharing jaringan internet. Keduanya dapat dicegah dengan tidak melakukan login dari komputer yang dishare. Namun kondisi negara ini di mana sulit mendapatkan akses internet pribadi yang murah menjadikan penggunaan komputer yang dishare sangat tinggi, seperti penggunaan warnet sebagai tempat untuk membuka situs jejaring sosial.

Di sinilah coba diterapkan steganografi untuk meningkatkan keamanan validasi ini.

II. LANDASAN TEORI

A. Steganography



Steganografi adalah suatu metode untuk menulis pesan rahasia dengan suatu cara yang membuat tidak ada orang, selain pengirim dan penerima yang dituju, mencurigai adanya pesan tersembunyi. Kata steganografi berasal dari Yunani yang berarti “tulisan terselubung” yang berasal dari kata *steganos* (στεγανός) berarti “tersembunyi atau terjaga” dan *graphein* (γράφειν) yang berarti “menulis”. Biasanya, pesan akan tampak seperti hal lain: gambar, artikel, daftar belanja, dan lain sebagainya, pada jaman dulu, pesan akan ditulis menggunakan tinta tak tampak di antara tinta biasa pada surat.

Kelebihan steganografi, dibanding kriptografi biasa, adalah pesan tidak menarik perhatian. Sebuah pesan terenkripsi –tidak peduli seberapa tidak terpecahkan- akan menarik perhatian, dan dapat menjadi kejahatan pada negara di mana enkripsi adalah ilegal. Oleh karena itu, di mana kriptografi melindungi isi dari pesan, steganografi dapat dikatakan melindungi pesan sekaligus juga pengirim dan penerimanya.

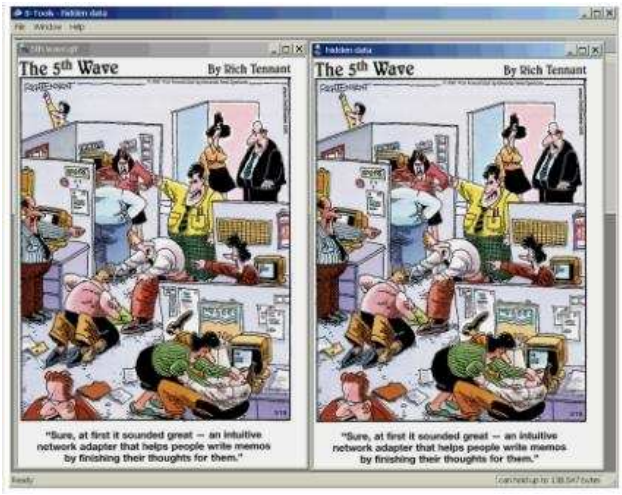
Steganografi paling pertama tercatat pada tahun 440 SM pada saat Herodotus menyebutkan mengenai 2 contoh steganografi pada *The Histories of Herodotus*. Demaratus memberi peringatan akan adanya serangan dari Yunani dengan cara menulisnya langsung pada bagian belakang sebuah *wax tablet*. Contoh kuno lainnya adalah Histiaeus, yang mencukur rambut budak kepercayaannya dan mentataokan sebuah pesan. Setelah rambutnya tumbuh pesan menjadi tersembunyi. Tujuannya adalah untuk merencanakan kudeta terhadap bangsa Persia.

Steganografi meliputi juga penyisipan informasi dalam data komputer. Dalam steganografi digital, komunikasi elektronik dapat meliputi kode steganografik dalam *transport layer*, seperti file dokumen, file gambar, program, atau protocol. File media adalah ideal untuk transmisi steganografik karena ukurannya yang besar. Sebagai contoh, seorang pengirim dapat memulai dengan sebuah file gambar kemudian mengubah warna setiap piksel ke-100 untuk merepresentasikan sebuah huruf dalam alfabet, sebuah perubahan yang sangat kecil sehingga orang yang tidak dengan sengaja mencari dapat dibilang tidak akan sadar.

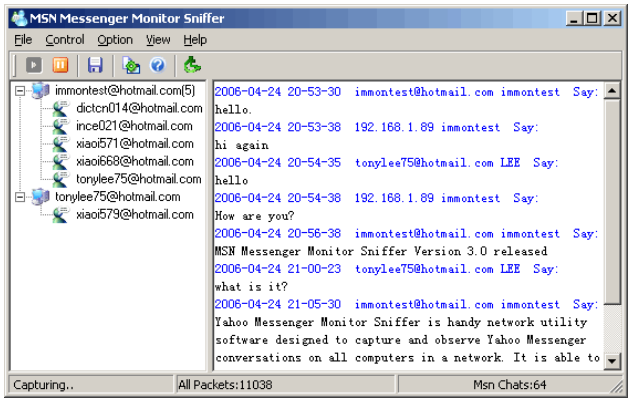
Steganografi modern diperkenalkan ke dunia pertama kali pada tahun 1985 dengan personal computer diaplikasikan pada persoalan steganografi klasik. Sekarang ini lebih dari 800 aplikasi digital steganography telah ditemukan oleh Steganography Analysis and Research Center. Teknologi steganografi digital yang diimplementasikan pada Steganopassword adalah teknologi menyimpan pesan pada bits terkecil dari gambar.

Dalam dunia komputer, mendeteksi sebuah paket yang terstegano disebut Steganalisis. Cara paling simpel untuk mendeteksi sebuah file yang dimodifikasi adalah dengan membandingkannya dengan file orsinilnya. Sebagai contoh, untuk mendeteksi informasi yang dipindahkan melalui gambar pada sebuah situs, seorang analis dapat melihat salinan asli dari materi yang ada dan membandingkannya dengan konten pada situs. Perbedaannya, dengan asumsi *carrier* sama, akan membentuk *payload*. Pada umumnya, menggunakan kompresi yang luar biasa tinggi membuat steganografi sangat sulit, namun tidak mustahil. Meskipun kesalahan pada waktu kompresi memberikan tempat bersembunyi untuk data, kompresi tinggi menurunkan jumlah data yang dapat digunakan untuk tempat bersembunyi *payload*,

membuat deteksi lebih mudah dilakukan.



B. Sniffer



Sniffer Paket (arti tekstual: pengendus paket — dapat pula diartikan 'penyadap paket') yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (*promiscuous mode*) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).

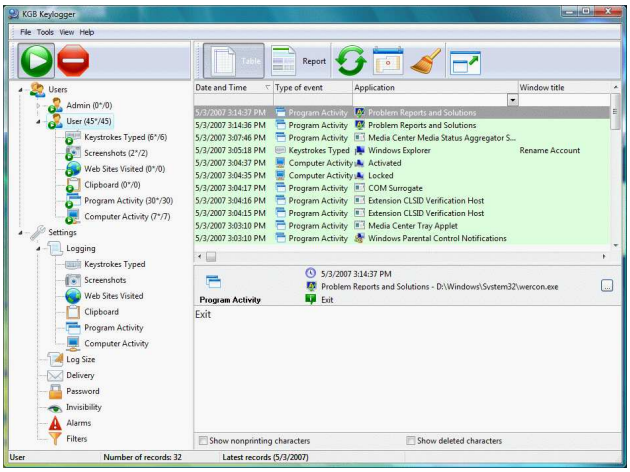
Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:

- Mengatasi permasalahan pada jaringan komputer.
- Mendeteksi adanya penyelundup dalam jaringan (*Network Intusion*).
- Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
- Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan password).
- Dapat digunakan untuk *Reverse Engineer* pada jaringan.

Penggunaan *sniffer* untuk meretas sistem validasi login terletak pada kemampuan *sniffer* untuk mendapatkan paket yang merupakan username dan password yang dikirimkan oleh user. Sebuah *sniffer* dapat dengan mudah mendapat username dan password serta situs yang dimasuki oleh seorang user.

Contoh : MSN Sniffer, Ace Password Sniffer, dsb

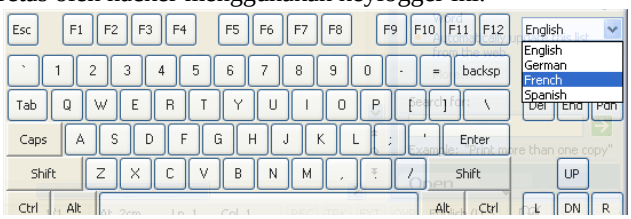
C. Keylogger



Keylogger merupakan sebuah perangkat baik perangkat keras atau perangkat lunak yang digunakan untuk memantau penekanan tombol keyboard. Sebuah *keylogger* biasanya akan menyimpan hasil pemantauan penekanan tombol *keyboard* tersebut ke dalam sebuah berkas log/catatan/rekaman. Beberapa *keylogger* tertentu bahkan dapat mengirimkan hasil rekamannya ke *e-mail* tertentu secara periodik.

Keylogger dapat digunakan untuk kepentingan yang baik atau bahkan bisa digunakan untuk kepentingan yang jahat. Kepentingan yang baik antara lain untuk memantau produktivitas karyawan, untuk penegakan hukum dan pencarian bukti kejahatan. Kepentingan yang buruk antara lain pencurian data dan *password*.

Keylogger dapat dihindari dengan menggunakan virtual keyboard atau on-screen keyboard. Karena prinsip dari keylogger adalah menyimpan aktifitas dari penekanan keyboard, virtual keyboard yang memvirtualisasikan fungsi keyboard dengan menggunakan mouse tidak dapat diretas oleh hacker menggunakan keylogger ini.



Contoh : Active Key Logger, Free Key Logger, dsb

III. STEGANOPASSWORD

Dengan melihat cara kerja kedua cara mencuri username dan password di atas, maka coba dirancang suatu metode yang tidak dapat diretas baik dengan *sniffer* maupun *keylogger*. Metode yang coba diterapkan adalah dengan penggunaan Steganopassword.

A. Metode

Pada Steganopassword user tetap diminta untuk memasukkan username dan password, yang berbeda di sini adalah password yang diminta harus berupa sebuah file gambar. File gambar yang dimaksud pertama-tama disisipkan password dengan menggunakan aplikasi pembuat steganografi, aplikasi seharusnya disediakan oleh situs yang bersangkutan sebab pendekripsian file Steganopassword haruslah dengan algoritma situs tertentu yang bisa saja berbeda antara tiap situs.

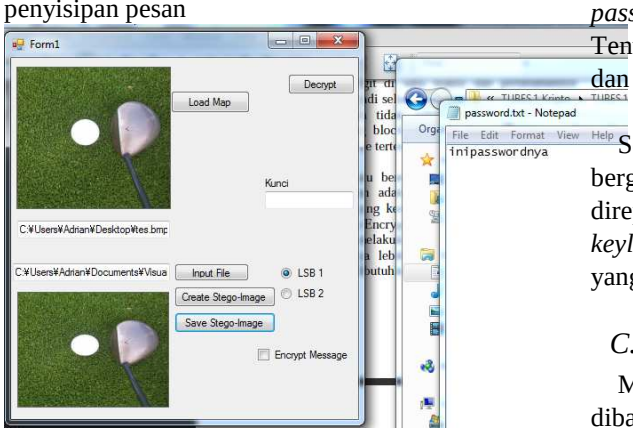
Setelah memasukkan username secara manual (bisa disediakan fitur virtual keyboard untuk meningkatkan keamanan terhadap *keylogger*) serta memasukkan Steganopassword, sistem validasi akan mendekripsi Steganopassword untuk memvalidasi user yang memasukkan.

Contoh di bawah ini menggunakan teori aplikasi steganografi yang diterapkan pada tugas besar 1 kuliah Kriptografi.

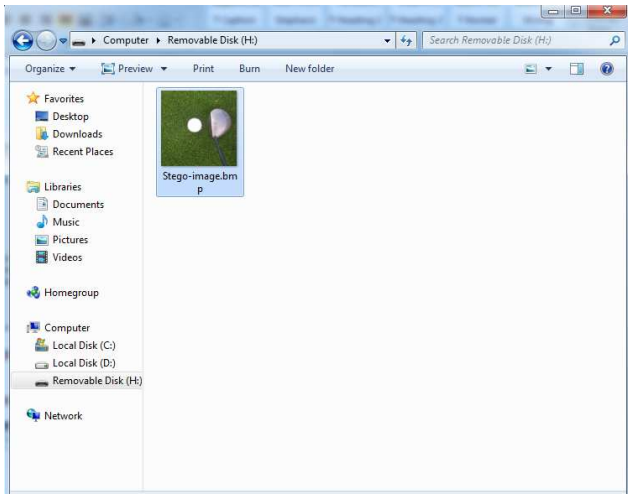
Teorinya adalah memasukkan pesan teks (password) ke dalam sebuah gambar dengan metode 1-bit atau 2-bit LSB, pada aplikasi Steganopassword, username digunakan sebagai kunci, kunci di sini berguna untuk membangkitkan *random number* yang berguna untuk melacak posisi pesan pada gambar.

Langkah-langkah yang diperlukan dalam realisasi penggunaan Steganopassword:

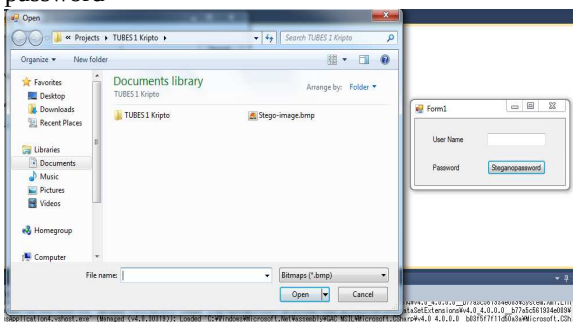
1. Pembuatan Steganopassword dengan aplikasi penyisipan pesan



2. Penyimpanan Steganopassword dalam media ekternal



3. Penggunaan Steganopassword sebagai validasi password



B. Konsep

Konsep Steganopassword ini adalah mencoba menghindari *sniffer* dan *keylogger*, dengan cara menyamarkan password sedemikian sehingga tidak terdeteksi oleh kedua metode.

Untuk menghindari *sniffer* karena file yang dikirimkan merupakan sebuah file gambar, dan *sniffer* tidak memiliki kemampuan untuk mendekripsi file gambar tersebut menjadi sebuah password, maka yang akan didapat oleh *sniffer* adalah data dari gambar yang sulit untuk dimengerti oleh *sniffer* bahkan mungkin hilang karena *password sniffer* mengubah file gambar menjadi string. Tentunya ini tidak akan berguna untuk meretas username dan password user yang bersangkutan.

Sementara *keylogger* pada hal ini akan hampir tidak berguna sebab tidak mungkin file gambar dapat direpresentasikan menggunakan keyboard, sehingga *keylogger* tidak akan mendapatkan aktifitas keyboard yang dapat membocorkan username dan password.

C. Kelebihan

Metode Steganopassword memiliki beberapa kelebihan dibandingkan dengan metode validasi biasa, yaitu:

- Aman terhadap aktifitas *keylogger*
- Aman terhadap aktifitas *sniffer*

- Tidak mungkin terjadinya kecurian informasi password secara aksidental

D. Kekurangan

Namun Steganopassword juga memiliki kekurangan, seperti:

- Merepotkan pengguna dengan harus membawa file gambar ketika login
- Meningkatnya waktu yang diperlukan dalam melakukan login

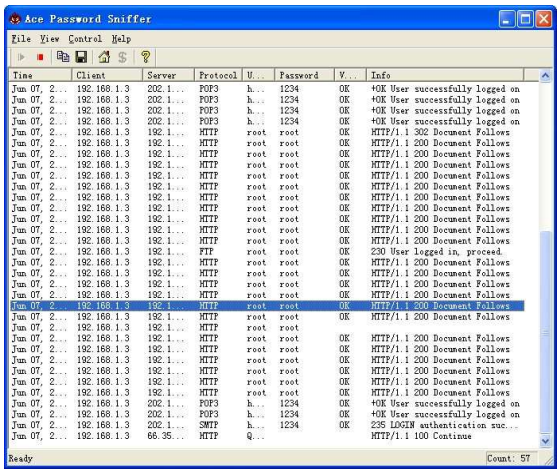
V. PENGUJIAN

Pengujian dilakukan dengan memasukkan Steganopassword dan melihat apa yang didapat menggunakan *sniffer* dan *keylogger*.

A. Sniffer

Pengujian dilakukan dengan aplikasi *AcePasswordSniffer* sebuah aplikasi *sniffer* untuk melihat paket yang dikirimkan oleh komputer

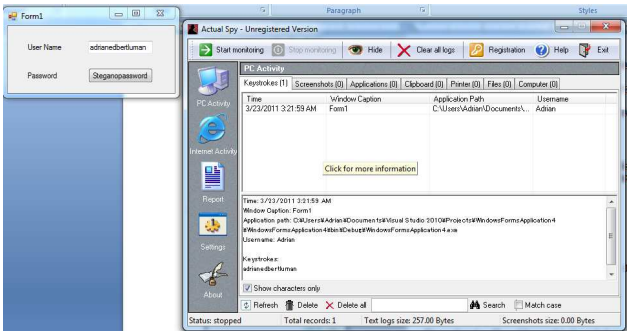
Sayangnya *AcePasswordSniffer* hanya mentrack paket yang menuju ke modem sehingga tidak dapat dilakukan pengujian dengan menggunakan aplikasi windows yang bekerja pada satu PC, namun seharusnya *AcePasswordSniffer* tidak menangkap file Steganopassword sebab tidak dianggap sebagai password.



Seperti dilihat pada gambar di atas *Ace Password Sniffer* menyimpan paket yang didapat dalam bentuk String.

B. Keylogger

Pengujian dilakukan dengan aplikasi *ActualSpy* sebuah aplikasi *keylogger* untuk melihat aktifitas yang dilakukan PC menggunakan keyboard



Bisa dilihat dari gambar di atas, *ActualSpy* berhasil mendapatkan username yang diketikkan oleh user namun tidak mungkin bisa mendapatkan aktifitas yang dilakukan user ketika mengupload file Steganopassword.

VI. KESIMPULAN DAN SARAN

Steganopassword memang masih memiliki kekurangan dibanding metode validasi biasa. Kekurangan terbesar adalah ketidak praktisan yang timbul karena harus menggunakan file gambar yang berasal dari media penyimpanan eksternal untuk melakukan login.

Namun tingkat keamanan Steganopassword, terutama terhadapa *sniffer* dan *keylogger* lebih baik dibanding menggunakan metode validasi biasa.

Perlu diadakan riset lebih lanjut mengenai perbandingan antara kekurangan dan kelebihan Steganopassword ini sebelum menjadikan Steganopassword pengganti metode validasi biasa yang sudah ada sekarang.

DAFTAR PUSTAKA

[1] R. Munir, "Diktat Kuliah IF5054 Kriptografi", Program Studi Teknik Informatika, Institut Teknologi Bandung, 2006.

[2] http://en.wikipedia.org/wiki/Steganography

[3] http://en.wikipedia.org/wiki/Sniffer

[4] http://id.wikipedia.org/wiki/Keylogger

[5] http://www.ilmuwebsite.com/seputar-hacking/tutorial-hacking/koleksi-63-keylogger-pilihan

[6] http://www.effetech.com/

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, 23 Maret 2011

ttd

Adrian Edbert Luman dan 13507057