Upravljanje i zaštita informacionih sistema - TrueCrypt

Vrsta: Seminarski | Broj strana: 30 | Nivo: Fakultet organizacionih nauka, Beograd

САДРЖАЈ

Увод

Шифровање (енг. encryption) обухвата математичке поступке модификације података такве да шифроване податке могу прочитати само корисници са одговарајућим кључем. Дешифровање (енг.decryption) је обрнут процес:шифровани подаци се помоћу кључа трансформишу у оригиналну поруку или датотеку.

Основни појмови:

Криптографија – наука о тајном писању (записивању), наука која се бави методама очувања тајности информација.Потиче од грчких речи kriptos (тајно,сакрити, скривено) i grafos (писати,писање).

Криптографски алгоритам – трансформише читљив текст P (plain text) у нечитљив текст C (crypted, chiphered text).

Криптоанализа- наука о добијању читавог текста P (или кључева...) на бази шифрованог текста

Напад – покушај криптоанализе

Компромитовање – добијање тајне без криптоаналитичких метода

Поверљивост (тајност) – превенција од неауторизованог приступа информацијама (обезбеђује приватност за поруке)

Интегритет (целовитост) – превенција од неауторизованог мењања информација (обезбеђује потврду да порука остаје непромењена)

Расположивост – превенција од неауторизованог онемогућавања приступа информацијама или ресурсима

Аутентификација – превенција од лажног представљања (идентификација извора поруке и верификација идентитета особе)

Криптосистем се дефинише као уређена петорка (P, C,
K, E, D), где је:

- P – скуп порука
- C – скуп шифрата
- K – скуп кључева
- E(P, K) → C – функција шифровања
- D(C, K) → P – функција дешифровања

Постоје две врсте криптографских алгоритама:

Симетрични – системи код којих су кључ за шифровање и дешифровање исти (цезарова шифра, вижнерова шифра,Playfair...)

Асиметрични – системи код којих су кључ за шифровање и дешифровање различити (RSA (Rivest, Shamir, Adleman),ElGamal)

1.Заштита фајлова на рачунарима

Постоји велики број фајлова на нашим рачунарима који садрже осетљиве податке.Ако оставимо ове фајлове незаштићене, тј. у нешифрованом облику, постоји опасност да они буду злоупотребљени, због чега је најбоље да ове фајлове шифрујемо.

Шифровање је процес у којем се оргиналне информације путем алгоритма трансформишу како би

биле нечитљиве свима осим онима који поседују лозинку. Један од бесплатних алата који нам са лакоћом омогућава да шифрујемо наше фајлове је TrueCrypt .
TrueCrypt је програм који испуњава већину критеријума напредне заштите и шифрирања фајлова, а оно што је најбитније је као што смо напред навели да је потпуно бесплатан.
Колико је битна заштита података појединостављемо на следећем примеру.Почетком деведесетих није било оволико рачунара као што их данас има.Рачунари су до пре само двадесет година били изузетно скупи и људи су водили рачуна о томе да им рачунар пре свега ради, тј.да се не поквари, док се о документима који су се у њему налазили много мање размишљало.Међутим, само двадесет година касније, тј. данас размишљања су дијаметрално супротна: компјутер је потрошна роба и да му нешто буде,односно у случају да се поквари нема великих трошкова што се тиче самог комјутера, јер се за релативно мали новац може купити нови.Значи компјутер је заменљив, међутим подаци похрањени у њему нису.Вредност комјутера је врло опипљива и може се изразити бројевима у некој валути, али вредност података је дословно речено непроценљива зато што је податке који су се скупљали 10 и више година немогуће надокнадити.