IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4656

Safety of Data in Computer Systems: Introduction to the Study of the Cryptography – Methods and Algorithms

Rômulo Cássio Reginaldo Bezerra and Aluízio Ferreira da Rocha Neto
Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte – FARN, Rua Prefeita Eliana Barros, Brazil
Tel: +55(84) 215-2918, Fax: +55 (84) 211-8688, rmurdock@mail.com, aluiziorocha@hotmail.com

ABSTRACT

The importance of the study of the cryptography feels in one moment in that the electronic trade grows exponentially in Internet and it is done necessary a middle of protecting the data that freely in Internet. This document offers a general vision of network security softwares and related methods for the professionals of network security of the present time. The approached topical principal will be: protection of networks through the cryptography and cryptographic softwares. We will present an abbreviation historical notes of the cryptography making a comparison with the systems of the present time.

INTRODUCTION

After September 11, 2001, the world understood that it lived under constant threat of some attack type. The concern with this new reality surpassed the governments' ambit and financial institutions and it also reached the organizations that noticed the significant increase of the threats and of the vulnerability the one that is exposed, mainly in what refers the discharge vulnerability of the digital atmosphere.

The need to protect your assets and to assure the continuity of the operations, it has been taking the companies they develop a system of administration of information security to implement controls based on analyses of the risks to the business and in legal and compatible requirements with the nature of your activity.

For your time, the users of information systems were more alert and cautious in the hour of accomplishing operations on-line.

In agreement with Módulo consulting (Módulo, 2002) of 547 Brazilian companies interviewees, 72% of those companies suffered some attack type to October of 2002. Of those, 19% had inferior loss the US$ 15 thousand, 8% had losses between US$ 15,000 and US$ 400,000 and 1% above US$ 400,000.

Another study of Gartner Group (Barbosa, 2002) showed that swindle them in stores on-line in 2001 they arrived to 700 million dollars.

For Santos (2002), one of the problems for the lack of safety of the companies, is the system administrators' unpreparedness that not always they are willing to install all the "patchs" and updatings that appear every day. The speed with that the technology moves forward and the easy access to the "hackware" in Internet is another added difficulty.

CRYPTOGRAPHY: AS EVERYTHING BEGAN

Before introducing to the study of the cryptography, we will have a fast vision on the history of the cryptography.

In agreement with Terada (2000), the cryptography flows of the words Greek "kriptó" that it means "hidden" and "logos" that means "word." Soon cryptography means hidden word.

The cryptography, in agreement with Burnett (2002) it is so old when the writing but it is not known for sure in that time the cryptography became used for ends of safety; what is known for sure it is that the cryptography began to be used for military ends. A classic example and one of the oldest cryptographic systems documented (Carvalho, 2002), it is Caesar's System, of the Roman emperor Julios Caesar. The system consisted of substituting a letter of the alphabet for an another in such a way that this substitution relationship was fixed; in this case the key ch is a whole number between 0 and 25 and each letter L it was encrypted using the following equation:

$L' = (L+Ch) \bmod 26$

and for decrypt it is had:

$L = (L'-Ch) \bmod 26$

This cryptography method is known as system of substitution word by word and it is shown extremely simple given that only have a maximum of 26 possible keys; although extremely fragile it was used with success during the empire.

As the Cryptography Works Today

The cryptography today is the half more used for the sending of secret information through insecure communication lines (Carvalho, 2001). Your use is going of safe e-mails to protocols of safety. Several techniques exist to use the cryptography efficiently but the key cryptography is one of the more used. For Terada (2000), key secretes of cryptography it is a mechanism that seeks to maintain the safety of what it was encrypted and of the user's only knowledge. It works as an additional protection to the cryptography.

According to Burnett (2002), one problem of this system is in the choice of the key that if it goes very easy or of easy deduction, it doesn't increase safety any and the algorithm will be easily "broken."

In agreement with Terada (2000), the systems of key cryptography are divided and, systems of symmetrical and asymmetric key; symmetrical when it uses the same key for encrypt and decrypt; asymmetric when the key that was used for encrypt is not necessarily made necessary for decrypt.

The cryptography of stronger symmetrical key today, meets in the level of 128 bits.

For understanding ends, we will see how the cryptography key works. See an example below with a key with three bits:

000 001 010 011 100 101 110 111

now, adding one more bit, we see that the number of possible keys is bent:

0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111

Breaks and Attacks in Cryptography

Several ways exist of breaking the cryptography. The algorithm can be attacked or to attack the cryptography key. For break of cryptography key, one of the attacks more used it is the attack of rude force.

Table 1. A worse scenery than the worst of the situations: How long an attack of rude force would take with relationship to the several key sizes (Burnett, 2002)

Bits	1% of the space of the key	50% of the space of the key
56	1 second	1 minute
57	2 seconds	2 minutes
58	4 seconds	4 minutes
64	4.2 minutes	4.2 hours
72	17.9 hours	44.8 days
80	190.9 days	31.4 years
90	535 years	321 centuries
108	140.000 millennia	8 million of millennia
128	146 billion of millennia	8 trillion of millennia

In agreement with Burnett (2002), a method of attack of rude force consists of trying all the possible keys until that the correct is identified. To proceed, a very simple algorithm of attack of rude force:

```
/ * Algorithm of Rude Force * /
1. Begin
      a. Y := 0;
      b. I := 0;
      c. Read (k);
      d. While (Y <> K) of the
                  i. Y := I +1;
      e. Write (“ The Key is: ”, Y);
2. end.
```

That method takes a long time in normal computers but computers exist created exclusively to break cryptographic systems. One of them is DeepCrack. A computer of the American government capable to test one billion keys a second (Terada, 2000).

For Burnett (2002), essentially 50% of the key are researched before being broken. To proceed, we have a table with a worse scenery than the worst of the situations with relationship at the time of an attack of rude force would take with relationship to the several sizes of the keys (see Table 1).

In fact, the technology of cryptography key has been advancing in a such way that is very unlikely that hackers get to break an alone key.

In recent challenge proposed by RSA Securities, they were necessary four years and more than 331 thousand computers working daily to decipher the secret key RC5-64 of 64 bits. In agreement with Alexandre Cagnoni, general manager of RSA Security in Brazil, RC5-64 has combinations of 18 million of trillion of keys. An alone hacker or in small group it would take many years the plus, or even some decades, to get to find the correct key. (Santos, 2002).

CONCLUSIONS

The security data in computers network it has been critical factor in the executives’ of IT calendar in the whole world. In fact, the technology has been moving forward to wide steps and it doesn’t get to be the largest problem. As it was seen, network’s administrators’ unpreparedness is that causes the largest index of attacks with success in the nets of computers; it doesn’t advance to place an algorithm with key of 512 bits if the used key is something like 123456.

In fact, it is quite unlikely that the size of symmetrical key surpasses the 512 bits; what generates a size of such big key that she cannot list in that document.

However the cryptography is not and nor it should be the only middle of maintaining secret data; it is just a tool as several other existent ones.

Is the alert so that the cryptography community and of safety of the information it announces telling your researches and the flaws found in the cryptography algorithms. The success of those tools depends of as they are explored.

REFERENCES

BARBOSA, Alexandre. Security e-business. Internet Business Magazine. São Paulo, Brazil: v.XVII, n195, jun. 2002., pg. 25/37.

BURNETT, Steve, PAINE, Stephen. Cryptography and security: The official guide RSA. Rio de Janeiro: Campus, 2002.

CARVALHO, Daniel Balparda de. Security data with cryptography: methods and algorithms. 2ed., Rio de Janeiro: Book Express, 2001.

MÓDULO, Security Magazine. 8th National research of information security. [online] Available in Internet through WWW.URL: http:// www.modulo.com.br/comum/docs file captured on November 05, 2002.

SANTOS, Teresa. Chances exist of winning the hackers. Information Week Brazil Magazine. São Paulo, Brazil: 12/04/2002, Y.04 N.83, P.27, DEC. 2002.

TERADA, ROUTO. Security data: Cryptography in computers networks. São Paulo, Brazil: Edgard Blücher, 2000.