KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 8, No. 2 (2018), p. 1 – 7

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

The possibilities of encryption information

Možnosti kryptovania informácií

Martin BOROŠ[1]

[1]*Department of Security management, University of Žilina, Slovakia*

The manuscript was received on 15. 11. 2018 and was accepted after revision for publication on 01. 12. 2018

Abstract:

Nowadays, information in various forms is highly desirable and oftentimes abusive. There are clearly several reasons, among which we could include digitizing data and transmitting information electronically. The reasons are to be helpful to the user on the one hand, in terms of facilitating both working and private life. On the other hand, however, the possibility of misuse of the transmitted information, which should only be addressed to the recipient, is created. From the above mentioned, the need for adequate protection of information in the company has resulted in the use of encryption or cryptography through which unauthorized persons have no access to information. With the development of information technologies, various standards of information encryption have been created, with an increasing interest in the protection and security of information. Encrypting information is transformed into an unreadable or unclear form, and its full meaning can only be obtained by using the key needed to decrypt content. The aim of the contribution is to clarify the meaning and possibilities of encryption with a practical example of encryption of information transmitted to the centralized protection desk.

Keywords: *information, encryption, security, protection, alarm transmission system.*

Abstrakt:

V dnešnej dobe sú informácie v rôznych podobách veľmi žiadaný a často krát aj zneužívaným aspektom. Dôvodov je jednoznačne niekoľko, medzi hlavné by sme mohli zaradiť digitalizáciu dát a prenos informácií prostredníctvom elektronickou formou. Spomínané dôvody majú byť užívateľom na jednej strane nápomocné, v rámci uľahčenia pracovného ale aj súkromného života. Z druhej strany sa však vytvára možnosť zneužitia prenášaných informácií, ktoré mali byť určené len príjemcovi. Zo spomínaného vyplynula v spoločnosti potreba patričného chránenia informácií pri ktorej sa využíva šifrovanie alebo kryptovanie pomocou ktorého nemajú k informácií prístup neoprávnené osoby. S vývojom informačných technológií vznikali rôzne štandardy kryptovania informácií so zvyšujúcim záujmom o ochranu a bezpečnosť informácií. Kryptovaním sa informácia pretransformuje do nečitateľnej alebo nejasnej podoby a jej plnohodnotný význam je možné získať

len pomocou použitia kľúča potrebného pre dekryptovanie obsahu. Cieľom príspevku je ozrejmenie významu a možností kryptovania s praktickým príkladom kryptovania informácie prenášanej na pult centralizovanej ochrany.

Kľúčové slová: *informácia, kryptovanie, bezpečnosť, ochrana, poplachový prenosový systém.*

Introduction

The security of the transmission of messages in alarm transmission systems against deliberate attempts to influence the transmission of information transmitted through an alarm transmission system is ensured by one of the following means:

- protection against substitution,
- securing information.

Information is a report, an indication, a value, a fact, a communication, or other data about an event, a phenomenon, an activity that reduces or eliminates ignorance, ignorance, or uncertainty in an area. It is also referred to as a type of knowledge or message that can be used to decide or improve an activity. Information is measurable and usually has its addressee. The fact is whether it removes the ignorance of the area or whether it is important for the recipient. The data is about process and element facts (e.g., measurement results). Data can take the form of letters, numbers, characters, and combinations. Data we call data in digital form.

Each information has two pages [1]:

1) Quantitative, respectively. syntactic, which expresses the composition of the message from the individual characters that allow the transmission of the message. This page is important for automated information processing.
2) Qualitative, respectively. semantic, which states:
   - the adequacy of the factual representation of the information,
   - usefulness of information for the recipient.

Information on privacy and property protection can be broken down into:

- situational,
- operational,
- directives.

1. Encryption

Encryption is a science of concealing the content of messages, and its name comes from the Greek cryptos which means hidden. Currently, cryptography is considered part of mathematics and computer science and is highly associated with computer security. The gradual development of cryptography resulted in the division of different types of cryptographic algorithms into several groups. The basic division consists of [2]:

- systematic cipher - mostly used with asymmetric. The use is that the open text is encrypted with a systematic key with random key generation. This is then encrypted by the public key of the asymmetric cipher, so decryption of the data can only be done by the owner of the secret, generated key.
- asymmetric ciphers.

The aim of cryptography is the security of information systems focusing on [3]:

- confidentiality - when transferring data and storing it on media,
- integrity - correctness of the content of the transmitted message,
- authentication - authentication.

Data encryption is the process by which unsecured electronic data is transferred using cryptography to data encrypted, legible only to the decryption key owner. Data encryption serves to protect against unauthorized abuse by an unauthorized person and is used to store data in transit as well. Data encryption is a type of cryptography that provides electronic data to protect the privacy of the owner.

By the word cipher or cryptography, we will refer to a cryptographic algorithm that converts a readable message or plain text into its unreadable form or ciphertext. The key is secret information without which the encrypted text cannot be read. At present, symmetric and asymmetric encryption, or their combination, are used [3].

Encryption and decryption requires knowledge of the secret information that the sender and the addressee know (ideally). This classified information is generally called the key. In practice, we recognize the so- weak keys, the use of which results in encryption in poor quality, for example, the original and encrypted text are similar. In case of a semi-weak key there is a direct relationship between open and encrypted text.

An important advancement in cryptology has been the invention of the Feisty Cryptosystem by means of which encryption is carried out in several in principle by the same steps sequentially applied to blocks of open text. At each step, only a transformation function that is arbitrary is changed and its output is dependent on the key. Decryption is very simple as it is enough to apply the encryption steps to the encrypted block in the reverse order. An example of an algorithm based on this principle is DES that was unbeatable at the time of its creation [4].

Encryption algorithms [3]:

- AES – Advanced Encryption Standard,
- 3-DES – Triple Data Encryption Algorithm,
- Blowfish,
- DES – Data Encryption Standard,
- DHE/DH – Diffie–Hellman key exchange,
- DSS – Digital Signature Algorithm,
- IDEA – International Data Encryption Algorithm,

- RC4 – Rivest Cipher 4,
- RSA – Rivest-Shamir-Adleman.

1.1. Symmetric encryption

Symmetric encryption is the procedure by which we uniquely encrypt the message with a fixed length key to encrypted text, and from the encrypted text we get the original message only if we know the encryption key used. Symmetric encryption consists of two parts, encryption and decryption, with [3]:

$$\mathbf{E\ (M,\ K) = T,}$$

$$\mathbf{D\ (T,\ K) = M.}$$

Where:

E - Encryption,
M - Administration,
K - Key,
T - Text,
D - Decryption.

The symmetric cipher consists of encryption and decryption that uses the same key. A symmetric cipher, sometimes called conventional, is an encryption algorithm that uses a single key to encrypt and decrypt. The essential advantage of symmetric cords is their low computational demands.

The disadvantage of the method is the need for increased security when selling the key and the impossibility of using it to sign / authenticate participants. The need for a key management mechanism if many people communicate with each other with different degrees of confidentiality (different keys for each pair) and need to change the keys after a certain period to change the Public Key Infrastructure, Web of Trust [5].

Symmetric encryption distribution [3]:

1) Substitute - replace the letter of the letter with a letter in another alphabet or letters of several alphabet,
   a. Mono-Alphabet - using one alphabet (eg Caesar's cipher),
   b. Polyalphabetic - Use of multiple alphabet.
2) Transposition - Shuffle text characters in different ways.

1.2. Asymmetric encryption

Symmetric encryption problem is in key transfer. The K key must be transferred through some medium, which has been one of the greatest priorities of international espionage in the past. It was no longer possible to transfer the key over an electronic channel that is very easy to remove. Physical transmission is, on the other hand, very slow, asymmetric encryption solves this problem very efficiently.

Asymmetric encryption is a series of procedures where we uniquely convert T1 text to T2 by using the Kn key (n = 1,2). It consists of two parts, the first part (encryption) converts the text M to the text T using the key K1 (usually called the public key). The second part (decryption) converts the text T to M, using the K2 key (most commonly referred to as the private key). The fact that K1 is not matched with K2 cannot be obtained by any mathematical procedure. The K2 private key is the key that only the person to whom the message is intended to hold. K1 is a public key that can be owned by anyone (the person can then download it online). Therefore, the M text encrypted with the K1 key can only be decrypted using a K2 key that has only the person to whom the message is addressed (it follows that the text T on the M text cannot be decrypted even by the person who encrypted it because it has no K2 private key, needed for this operation) [3].

For asymmetric encryption, only one key is not used, as is common in the so-symmetric encryption, but two keys are used. When the information is encoded with one key, it can only be decrypted by the other and vice versa. This means that if we encode something with one key and we do not have one, we will not get the original message. The algorithm's security (i.e., the time at which it is possible to break the algorithm and reach the original message without knowing the second key) depends clearly on the length of the key. This is now between 512 and 2048 bits, with the 1024-bit key today being considered real-time in real-time using current computer performance.

With the progressive increase in computer performance, the key length will gradually increase to maintain the same security of information transmission. These two keys are equivalent to the algorithm. One of them is called the so-called public key and the other private key. The public key can be made available to anyone who asks for it, but the private key must be kept well.

2. Advanced encryption standard

Advanced Encryption Standard, AES, is an advanced cryptographic standard used in security technology. AES is also known under its original name Rijndael, which is a specification for cryptography of electrical data set by the American National Institute for Standardization and Technology in 2001.

The AES cryptographic cipher is based on a principle that has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Thus, the encrypting system works with a 4x4 nut. The algorithm described by AES is a symmetric key algorithm, which means that the same key is used to encrypt and decrypt data [5].

The key size used for the AES cipher specifies the number of iterations of the transformation circles that convert the input, called plaintext, to the final output, which is called encrypted text. The number of repetition cycles is as follows:

- 10 repetition cycles for 128-bit keys,
- 22 iteration cycles for 192-bit keys,
- 14 iteration cycles for 256-bit keys.

2.1. Ademco Contact ID

Ademco Contact ID is the digital communication format used in electrical security systems to transmit alarm messages from central offices located in protected objects to centralized protection counters. The Contact ID has a fixed format and content of the individual alarm messages. The centralized protection counter is a transmitted tone and contains 15 characters. Hex numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E are used for the transmission [6].

ACCT MT QXYZ GG CCC S

Where:

ACCT - 4 numbers identify the object,
MT - Administration format. It is checked that the message is in the Contact ID format - 18/98. Newly produced centralized protection counters accept both values, older may be inconsistent with mark 98,
Q - defines the type of event:
1 - new event, alarm, opening,
3 - restoration or closure,
6 - the previously transmitted state that persists.
XYZ - 3 event numbers,
GG - subsystem numbers,
CCC - zone, user,
S - control report.

Conclusion

The aim of the paper was to point out the need to use cryptographic standards to protect not only transmitted information. In the contribution, the basic concepts of cryptography were elucidated, along with examples and basic divisions.

Subsequently, we focused on the AES cryptographic standard, which is one of the most challenging in security technology. In its definition, we focused mainly on the basic principle of operation, focusing on the number of cycles and repetitions for each key size. As a practical example of the encrypted information, we used the transcript of the alarm message transmitted to the centralized protection counter. Report encryption was performed using the Ademco Contact ID standard, which is currently the most used in alarm transmission systems.

It is important for every user to be aware of what value they can now have and what to do to protect their privacy.

Acknowledgement

This work was supported by the Internal Grant Scheme of Faculty of Security Engineering, University of Zilina from the grant no. IGP 201813 *Experimental testing of the reliability of the alarm transmission system.*

References

[1] LOVEČEK, T., VEĽAS, A., ĎUROVEC, M. *Bezpečnostné systémy: poplachové systémy*. Žilina: Žilinská univerzita v Žiline, 2015. 230 p., ISBN 978-80-554-1144-6.

[2] VEĽAS, A.: *Poplachové systémy - Poplachové prenosové systémy a zariadenia.* Žilina: Žilinská univerzita, 2015. 137 p., ISBN 978-80-554-1134-7.

[3] ENCRYPTION, 2017, [on line] [cit 5-11-2018] avaible from: https://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=19&ved=0ahUKEwi73v2_lOnXAhWNHRQKHVdBBW44ChAWCF0wCA&url=http%3A%2F%2Fwww.spseke.sk%2Fweb%2Fsviantek%2Fdownload%2F4_pos_teo%2F15_kryptovanie.ppt&usg=AOvVaw1rid5eXaptJhRBQT5_86H8

[4] GUTTEN, M., JANURA, R., SEBOK, M., KORENCIAK, D., KUČERA. M. *Measurement of short-circuit effects on transformer winding with SFRA method and impact test*, Metrology and measurement systems, 2016.

[5] BRVNIŠŤAN, M., KAMPOVÁ, K., LOVEČEK, T., SIVÁKOVÁ, L., VEĽAS, A. *Počítačová kriminalita.* Riešenie krízových situácií v špecifickom prostredí, Žilina, 2018.

[6] DIGITAL COMMUNICATION STANDARD - ADEMCO ® CONTACT ID PROTOCOL - FOR ALARM SYSTEM COMMUNICATIONS, 2010, [on line] [cit 5-11-2018] avaible from: http://www.technoimport.com.co/Producto/pdfs/ADEMCO%20-%20DC05_Contact_ID.pdf

Author:

[1]**Martin Boroš –** University of Zilina, Faculty of Security Engineering, Zilina, Department of Security management, Univerzitná 8215/1, 010 26 Žilina, Slovakia, martin.boros@fbi.uniza.sk