Proceedings of the 2013 Federated Conference on
Computer Science and Information Systems pp. 659–662

A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques

Georgiana Mateescu
Polytechnic University of Bucharest,
Splaiul Independenței 313, Bucharest, Romania,
Email: georgiana.mateescu@gmail.com

Marius Vladescu
Polytechnic University of Bucharest,
Splaiul Independenței 313, Bucharest, Romania,
Email: vladescumariusnicolae@yahoo.com

***Abstract*—Information protection is one of the most important issues in every domain, especially when we are talking about enterprises. Information safety can be translated into three key terms: integrity, availability and data protection. There is a great number of means used in order to achieve the three objectives simultaneously. The most popular is cryptography because it offers a lot of techniques which nowadays are impossible to fail. In this paper we want to prove their efficiency by comparing the different types of crypto algorithms and by presenting their weaknesses and strengths. In order to maximize the benefits of the crypto techniques, we propose a hybrid approach that combines three crypto algorithms.**

I. Introduction

WHEN we are talking about information security we refer to it as the mean we use to protect our information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The main concepts that a security system has to respect are: confidentiality, integrity, availability and authentication. These concepts represent the information security goals and must be achieved by every security system that aims to be functional. Most security systems use cryptography because it offers various algorithms and techniques practically impossible to break because of their complexity. Cryptography, not only protects data from unauthorized access or alteration, but it can also be used for user authentication. There are three main types of cryptographic algorithms used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions (Fig. 1).

In this paper, we will analyze these three ciphers: symmetric, asymmetric and hash function. After we present each of them with their strengths and weaknesses we will point out the main attacks that an efficient security system has to face in each case.

To conclude, we propose a hybrid approach of the presented cryptography techniques which combines them for taking benefits from all of their strengths and tries to reduce as much as possible the weakness of one technique with the advantages of the other, in the following manner:

- The original message's message digest is digitally signed (the digital signature uses RSA algorithm)
- Symmetrical cipher is used to code the original message (AES algorithm). The secret key is obtained using a key generator and it is periodically changed.
- The private key used for symmetric cipher is coded using also RSA algorithm, but with different keys.
- The coded private key is attached to the encrypted message together with the digital signature

These techniques will be incrementally introduced and combined into a unitary security system for small and medium enterprises. The purpose of this system is to face the vulnerabilities and threats these enterprises might encounter, by ensuring all the security components in the company's information flow.

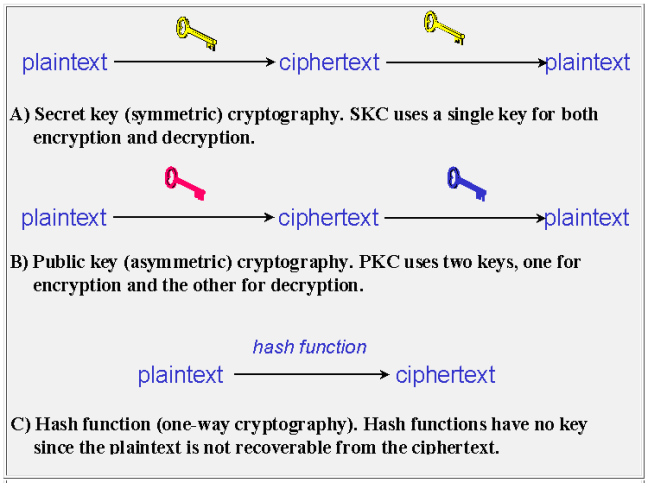

Fig. 1 The main three Cryptography Techniques [1]

II. Theoretical Background

A. Symmetric cryptography

This kind of cryptography uses a single key for both encryption and decryption, and it is also called secret key cryptography (SKC) [1]. This technique works by the following principles:

1. The plaintext is encrypted with the key and the ciphertext is sent to the receiver
2. The receiver uses the same key to decrypt the ciphertext and recover the plaintext.

978-1-4673-4471-5/$25.00

The key is a set of rules, and both the sender and the receiver must know the key in order to use the technique.

The most known secret key cryptography schemes are stream ciphers and block ciphers. The stream ciphers generate a sequence of bits used as a key called a keystream, and the encryption is accomplished by combining the keystream with the plaintext. This is usually done with the bitwise XOR operation. The keystream can be independent of the plaintext and ciphertext, in which case the stream cipher is synchronous, or it can depend of the data and its encryption, in which case the stream cipher is self-synchronizing. A block cipher transforms a fixed-length block of plaintext into a block of ciphertext of the same length. The same secret key is used for the decryption by applying the reverse transformation of the ciphertext block [2].

B. Asymmetric (Public Key) Cryptography (PKC)

This technique requires two types of keys: one to encrypt the plaintext and one to decrypt the ciphertext, and it doesn't work without one or another. It is called asymmetric cryptography because it is used a pair of keys: one is the public key that can be advertised by the owner to whoever he wants, and the other one is the private key and it is known only by the owner. The most common public key algorithm is the RSA algorithm, used for key exchange, digital signatures, or encryption of small blocks of data. It uses a variable size key and a variable size encryption block. The security of the RSA algorithm is based on the factorization of very large numbers. Two prime numbers are generated by a special set of rules, and the product of these numbers is a very large number, from which it derives the key-set [3].

C. Hash Functions

A hash function offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages. MD5 and SHA1 are algorithms for computing a fingerprint of a message or a data file. SHA-1 is described in the ANSI X9.30 standard and produces a 160-bit (20 byte) message digest. It is slower than MD5, but it has a larger digest size, which makes it stronger against brute force attacks. The advantage of MD5 is that it can be implemented faster, due to its 128 bit (16 byte) message digest [4].

III. Threats and Vulnerabilities

The main dangers an enterprise information system faces can be divided into:

- Threats –potential danger to information resources
- Vulnerabilities – weakness in application systems, network, business process or management procedures

The attacks that cryptography based security systems may suffer are dived into:

- Cyphertext-only - attempt to recover plaintext from encrypted text sent in the message.
- Known-plaintext - attempt to discover the key used when the analyst has access to the plaintext of the encrypted message.
- Chosen-plaintext same as Known-plaintext attack, but the analyst gets to choose the known plaintext.

A. Symmetric cryptography (secret key)

Although is the strongest technique that cannot be practically broken if we choose a proper complexity for the secret key, the symmetric crypto algorithms have to face a big threat in order to achieve its benefits: to safely transmit the secret key to the other part of the communication – where the decryption process is made.

Depending of the symmetric type of cipher, the usual attacks are as followed [5]:

- Block Cipher: shortcut attacks and brute force attacks. The shortcut attacks try to minimize the computational complexity required to find the correct key by exploiting the analytical and statistical characteristics of the algorithms. The most used shortcut attacks are differential cryptanalysis. The brute force attacks try one possible encryption key after another to obtain information on the correct key and/or the plaintext (For triple DES, both two-key and three-key triple DES has already been academically broken).
- Stream Cipher: its security depends on the pseudo-random number generator. If the pseudo-random numbers can be efficiently predicted from the past numbers, then the algorithm will be easily broken.

B. Asymmetric cryptography (public key)

The possible attacks on RSA are [6]:

- Searching the message space - if the message space is small, then the attacker could simply try to encrypt every possible message block, until a match is found with one of the ciphertext blocks. In practice this would be an insurmountable task because the block sizes are quite large.
- Guessing *d* - a known ciphertext attack (The attacker knows both the plaintext and ciphertext and he tries to find out the private part from the key)
- Cycle attack – it is the same as "Guessing *d*", but the coded text it is encrypted repeatedly until the original text is obtained. This number of re-cycles will decrypt any ciphertext.
- Low exponent
- Factoring the Public Key – it is considered to be the most efficient attack

C. Hash function (one way cryptography)

In the hash function case, the main vulnerability is the high probability of collisions appearance. Collisions represent the cases when two different inputs, using the same

hash function, generate the same output and therefore can be easily exploited.

In February 2005, Wang, Yin, and Yu [7] published research results which concluded that SHA-1 collisions can be found with the computational complexity equivalent to 2^{69} hash function operations. In addition, Wang, Yao, and Yao claimed that SHA-1 collisions can be found with the computational complexity equivalent to 2^{63} hash function operations.

IV. RELATED WORKS

Nowadays, small and medium enterprises use different techniques in order to achieve information protection. Some of them are based on cryptography [8, 9], others on PKI [10, 11]. All these architectures ensure a certain level of security that could be sometimes too small for the threats and the vulnerabilities that they have to face.

We propose a hybrid approach that wants to offer a complex solution with the following characteristics:

- Unified system – all the crypto techniques are combined to solve each other's threats and weaknesses
- Structured system – encapsulating different types of ciphers to maximize the efficiency

V. HYBRID ENCRYPTION SYSTEM

Data encryption is an important element of an organization's response to security threats and regulatory mandates. The enterprises are facing the fact that while encryption is not difficult to achieve, managing the associated encryption keys across their lifecycle quickly becomes a problem that creates a new set of security vulnerabilities and risks. The administration of keys must itself have built-in protection against internal maliciousness.

Encryption resources such as keys, hash algorithms, certificates, and digital signatures are dynamic and fluid. They must be changed, cycled, or renewed regularly. Furthermore, they must be archived under time-based management so that they would be available for retrieving.

By combining different cryptography techniques, this approach offers a solution for various weaknesses that must be faced in a security crypto system including:

- Key encryption management: key generator, key storage, key transmission
- Computing time
- Ensure all the security goals: integrity, availability, authentication and confidentiality

This crypto security system ensures (Fig. 2):

- Data integrity – using hash function
- Authentication and authenticity – using digital signature (DSA – asymmetric cryptography)
- Data confidentiality – using AES (Advanced Encryption Standard – symmetric cryptography algorithm)

A. Digital signature

For digital signature we can use RSA algorithm or DSA algorithm. In RSA algorithm, the message digest (the

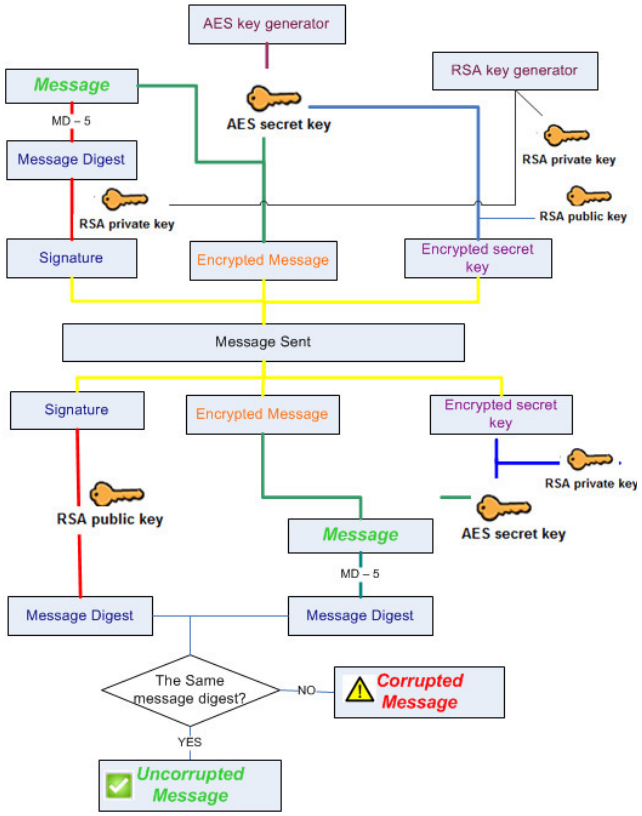

Fig. 2 Encryption schema

message hash) is encrypted with the RSA private key. This encryption represents the signature and it is attached to the message. It is obvious that this approach is impractical because:

- The ciphertext signature is the same size as the corresponding plaintext, so the messages sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors, so network and computer performance can be significantly degraded.
- Encrypting the entire contents of information produces large amounts of ciphertext, which can be used for cryptanalysis attacks, especially plaintext attacks (where certain parts of the encrypted data, such as e-mail headers, are known beforehand to the attacker).

National Security Agency developed DSS (Digital Signature Security Standard) which defines Digital Signature Algorithm. This algorithm is similar to RSA, but it does not encrypt message digests with the private key/ decrypt the message digest with the public key. Instead, DSA uses mathematical functions to generate a digital signature composed of two 160-bit numbers that are derived from the message digest and the private key. DSA uses the public key to verify the signature, but the verification process is more complex than RSA. DSA requires the use of the SHA-1 message digest function to ensure strong digital signatures and because of that and of the verification process, RSA digital signature

process generally provides better overall performance. Beside that DSA it never used to encrypt the message (for example you cannot use DSA to transmit the secret key of a symmetric cryptography algorithm).

Taking in count all these factors we will use RSA digital signature together with a RSA key generator – an algorithm used to generate secure RSA private and public keys.

B. Hash function

We use MD5 as a hash function hash function because it is faster than SHA – 1. Although it is weaker than SHA -1, we consider that the computing time is an important aspect which has to be optimised as much as possible.

C. Rijndael AES – symmetric encryption

AES algorithm has the following steps:

- Key generation
- Message encryption/decryption
- Key transmission: key encryption/decryption

Key generation is made using a cryptographically secure pseudo random number generator. We chose PRNG1 core because it is secure in wireless communications, RFID, Smart cards, electronic financial transactions. The key management system also includes the necessity of secure servers used for the key archiving and storage under time-based management so that historic data availability is ensured.

Message encryption is made using the generated key and Rijndael AES (Advanced Encryption Standard) algorithm. We chose this technique because, according to NIST, it has better security and efficiency characteristics than DES. Rijndael was designed based on the following three criteria [13]:

- Resistance against all known attacks;
- Speed and code compactness on a wide range of platforms;
- Design simplicity

Message decryption is made by the receiver using the same secret key as the sender.

Key transmission includes:

- Secret key encryption using RSA private key (generated by the key generator)
- Attach to the sent message the encrypted secret key

For the secret key transmission, we chose the most usually algorithm RSA because the practise has proved the fact that this technique successfully faces all the threats.

VI. Conclusions

Today's business environment is compliance-driven, competitive and increasingly fraught with from financially motivated hackers and frustrated employees. This creates a mounting demand for effective, practical, automated and risk-mitigating ways to manage keys throughout their lifecycle, so that only authorized users are granted access and the unauthorized user are thwarted. User and application access to these resources must be controlled, managed and audited so that authorized access is quick and reliable, all while preventing malicious attacks.

A strong crypto system together with a secure Key encryption management system can ensure all security goals. The combination of different cryptography algorithms provide a maximized efficiency, correcting or compensating each other's weaknesses.

VII. References

[1] Gary C. Kessler, *An overview of Cryptography*, 28 April 2013 http://www.garykessler.net/library/crypto.html

[2] RSA Laboratories- Chryptographic tools; section 2.1.5. unpublished; http://www.rsa.com/rsalabs/node.asp?id=2174

[3] Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ȚĂPUȘ ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatica Economica, nr. 2(30)/2004

[4] Arash Partow –"General Purpose hash Function Algorithms"

[5] Masashi Une and Masayuki Kanda, "Year 2010 Issues on Cryptographic Algorithms", Discussion Paper No. 2006-E-8, IMES, C.P.O BOX 203 Tokyo, 100-8630 Japan

[6] Prof. Patrick McDaniel, Network and Security Research Center Department of Computer Science and Engineering Pennsylvania State University, University Park PA – "Public-Key Cryptography and Attacks on RSA", 2010

[7] X. Wang, and B. de Weger, "Colliding X.509 Certificates," Cryptology ePrint Archive, 2005 (available at http://eprint.iacr.org/2005/067).

[8] Rodrigues, J. Roberts (2007). "System security and personal help data protection"

[9] Gregory Braun –" Crypto 2000" (*For Small to Medium Businesses*)

[10] Information Technology and Organizations: "Trends, Issues, Challenges and Solutions", VOLUME 1, 2003 Information Resources Management Association, International Conference,Philadelphia, Pennsylvania, USA,May 18-21, 2003

[11] Ki Woong Park, Hyun Jin Choi, and Kyu Ho Park-"An Interoperable Authentication System using ZigBee-enabled Tiny Portable Device and PKI", Internation Conference on Next Generation PC

[12] http://technet.microsoft.com/en-us/library/cc962021.aspx

[13] Daemen, Joan; Rijmen, Vincent. "AES Proposal: Rijndael" Document version 2, 1999