IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

A Study of Different Methods of Attacking and Defending Cryptosystems

Manjula G[1], Dr. Mohan H.S[2]

Dept of ISE, SJBIT, Bangalore, India[1,2]

Abstract: Encryption techniques have been utilized for a large number of years and, in this way, they are being capable of protecting sensitive data and this has been of incredible intrigue. As the privacy of our secrets have expanded, so have the technological innovations used to secure them. One of the key objectives of the individuals who need to keep confidential data secure is to keep ahead of the techniques used by the attackers. These assaults pose a genuine risk to the security of cryptographic modules. In outcome, cryptographic executions must be assessed for their resistivity against such assaults and the fuse of various countermeasures must be considered. This paper overviews the strategies and methods utilized in these assaults, the damaging impacts of such assaults, the countermeasures against such assaults and assessment of their achievability and materialness.

Keywords: Cryptography, attacks, Differential cryptanalysis, Linear cryptanalysis.

I. INTRODUCTION

In this rapidly changing Digital epoch, the means of communicating through multimedia components is very demanding and needs topmost security. Various data formats like text, multimedia etc is transmitted using different networking paradigm. Securing information on the system has turned out to be critical in this E-Commerce world. PC security is picking up significance and different strategies have been devised to ensure secret and vital data in the E-exchanges. Cryptography plays a critical role in the safety of information. It empowers us to store sensitive and confident data or transmit it over electronic systems so that unauthorized persons are denied access. Security in networking is based on Cryptography (a word with Greek origins, means “secret writing”), the science and art of transforming messages to make them secure and immune to attack [1]. Cryptography refers to the study of the techniques and methods used to hide data, and encryption is the process of disguising a message so that its meaning is not obvious. Similarly, decryption is the reverse process of encryption. The original data is called clear text or plaintext, and the encrypted data is called cipher text. Sometimes, the words encode/encipher and decode/decipher are used in the place of encrypt and decrypt. A cryptographic algorithm is commonly called a cipher. Cryptanalysis is the science of breaking cryptography, thereby gaining knowledge about the plaintext. The amount of work required to break an encrypted message or mechanism is call the work factor. Cryptology refers to the combined disciplines of cryptography and cryptanalysis. Cryptography is one of the tools used in information security to assist in ensuring the primary goals of confidentiality, integrity, authentication, and non-repudiation.

Cryptography Goals

Cryptographic method is used to achieve many goals and some of the goals are as follows:
1. Authentication: it is a process of giving identity to someone to access particular resource using the keys.
2. Confidentiality: It is most important goal of cryptography, which ensure that nobody understand the message except the one who has the cipher key.
3. Data Integrity: It is the process of ensuring that nobody is allowed to alter the transmitted message except the party who is allowed to do so.
4. Non-Repudiation: Ensure that neither the sender nor the receiver of the message should be allowed to deny the transmission of the message.
5. Access Control: Ensure that only the authorized parties are able to access the transmitted message.

Some of the things a cryptanalyst needs to be successful are:

- Enough cipher text
- Full or partial plaintext
- Known algorithm
- Strong mathematical background
- Creativity
- Time, time, and more time for analysis
- Large amounts of computing power

Copyright to IJARCCE
DOI10.17148/IJARCCE.2017.6570

Motivations for a cryptanalyst to attack a cryptosystem include:

- Financial gain, including credit card and banking information
- Political or espionage
- Interception or modification of e-mail
- Covering up another attack
- Revenge
- Embarrassment of vendor (potentially to get them to fix problems)
- Peer or open-source review
- Fun/education (cryptographers learn from others' and their own mistakes)

Classification of Cryptography algorithms

Cryptography Algorithms can be classified into two parts:

- **Symmetric cryptography**

This type of cryptography practices only one key for both encryption and decryption, and it is also called secret key cryptography [6]. This technique works by the following principles:
1. The plaintext is encrypted with the key to produce cipher text and it is sent to the receiver.
2. The receiver uses the same key to decrypt the cipher text and finds the original plaintext.

In Symmetric key cryptography both the sender and the receiver must know the same key in order to use the technique. In decryption, same secret key is used by applying the reverse transformation of the cipher text block and original plain text is produced [7]. Some examples of symmetric key cryptography include DES, IDEA, and RC4.

- **Asymmetric Cryptography (PKC)**

This technique requires two types of keys: one to encrypt the plaintext and one to decrypt the cipher text, 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. 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 [8]. Some examples of symmetric key cryptography include RSA and ECC.

Types of Keys

Most algorithms use some form of secret key to perform encryption functions. There are some differences in these keys that should be discussed.

1. **Private/Symmetric**. A private, or symmetric, key is a secret key that is shared between the sender and receiver of the messages. This key is usually the only key that can decipher the message.
2. **Public/Asymmetric**. A public, or asymmetric, key is one that is made publicly available and can be used to encrypt data that only the holder of the uniquely and mathematically related private key can decrypt.
3. **Data/Session**. A symmetric key, which may or may not be random or reused, is used for encrypting data. This key is often negotiated using standard protocols or sent in a protected manner using secret public or private keys.
4. **Key Encrypting**. Keys that are used to protect data encrypting keys. These keys are usually used only for key updates and not data encryption.
5. **Split Keys**. To protect against intentional or unintentional key disclosure, it is possible to create and distribute parts of larger keys which only together can be used for encryption or decryption..

II. ATTACKS ON CRYPTOSYSTEMS

This section is really split up into two classes of attack: **Cryptanalytic attacks** and **Implementation attacks**. The former tries to attack mathematical weaknesses in the algorithms whereas the latter tries to attack the specific implementation of the cipher (such as a smartcard system).

Attacks on cryptographic systems can be classified under the following threats:

- Interception
- Modification
- Fabrication
- Interruption

In the present era, not only business but almost all the aspects of human life are driven by information. Hence, it has become imperative to protect useful information from malicious activities such as attacks. Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be **passive** or **active.**

DOI10.17148/IJARCCE.2017.6570

Passive Attacks

The main goal of a passive attack is to obtain **unauthorized access to the information**. For example, actions such as intercepting and eavesdropping on the communication channel can be regarded as passive attack as illustrated in Figure 1.

These actions are passive in nature, as they neither affect information nor disrupt the communication channel. A passive attack is often seen as stealing information.

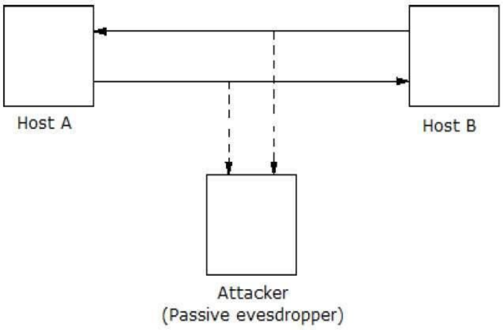

Figure 1 : Passive attack

Active Attacks

An active attack involves changing the information in some way by conducting some process on the information as shown in Figure 2. For example,

- Modifying the information in an unauthorized manner.
- Initiating unintended or unauthorized transmission of information.
- Alteration of authentication data such as originator name or timestamp associated with information
- Unauthorized deletion of data.
- Denial of access to information for legitimate users (denial of service).

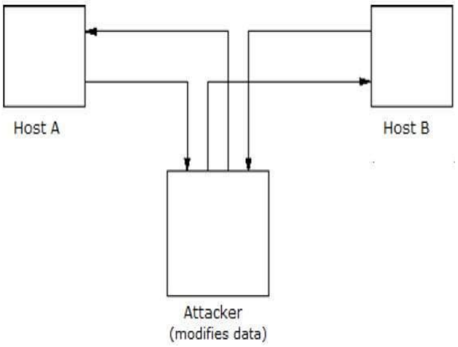

Figure 2 : Active attack

The following attacks can refer to either of the two classes (all forms of attack assume the attacker knows the encryption algorithm):

• **Ciphertext-only attack**: In this attack the attacker knows only the ciphertext to be decoded. The attacker will try to find the key or decrypt one or more pieces of ciphertext (only relatively weak algorithms fail to withstand a ciphertext-only attack).

• **Known plaintext attack**: The attacker has a collection of plaintext-ciphertext pairs and is trying to find the key or to decrypt some other ciphertext that has been encrypted with the same key.

• **Chosen Plaintext attack**: This is a known plaintext attack in which the attacker can choose the plaintext to be encrypted and read the corresponding ciphertext.

• **Chosen Ciphertext attack**: The attacker has the able to select any ciphertext and study the plaintext produced by decrypting them.

• **Chosen text attack**: The attacker has the abilities required in the previous two attacks.

The following terminology is also useful to know [2]:

• An encryption scheme is **unconditionally secure** if the cipher text generated does not contain enough information to determine uniquely the corresponding plaintext no matter how much cipher text is available or how much computational power the attacker has. With the exception of the one time pad, no cipher is unconditionally secure.

DOI10.17148/IJARCCE.2017.6570

• The security of a **conditionally secure** algorithm depends on the difficulty in reversing the underlying cryptographic problem such as how easy it is to factor large primes. All ciphers other than the one-time pad fall into this category.

An encryption scheme is said to be **computationally secure** if:
1. The cost of breaking the cipher exceeds the value of the encrypted information
2. The time required to break the cipher exceeds the useful lifetime of the information.

III. CRYPTANALYTIC ATTACKS

All forms of cryptanalysis for symmetric encryption schemes are designed to exploit the fact that traces of structure or pattern in the plaintext may survive encryption and be discernible in the ciphertext. Cryptanalysis of public-key schemes proceeds from a fundamentally different premise, namely that the mathematical properties of the pair of keys may make it possible for one of the two keys to be deduced from the other. In this section we will only be concerned with three main attacks. Two of them (Differential and Linear cryptanalysis) are used to attack block ciphers whereas the third (birthday attack) is used to attack hash functions.

Differential cryptanalysis

One of the most significant advances in cryptanalysis in recent years is differential cryptanalysis. Although this appears to have been discovered at least 30 years ago it was not reported in the open literature until 1990. The first published effort appears to have been the cryptanalysis of a block cipher called FEAL. This was followed by a number of papers by Biham and Shamir, who demonstrated this form of attack on a variety of encryption algorithms and hash functions. The most publicised results for this approach have been those that have application to DES. Differential cryptanalysis is the first published attack that is capable of breaking DES in less than 255 complexity. The scheme can successfully cryptanalyze DES with an effort of 247, requiring 247 chosen plaintext (hence it is a chosen plaintext attack). Although 247 is certainly significantly less than 255, the need to find 247 chosen plaintexts makes this attack of only theoretical interest. Apparently this attack was known at the time DES was being designed and played a large part in the design of DES.

Linear Cryptanalysis

A more recent development is linear cryptanalysis that was presented by Mitsuru Matsui [3]at Eurocrypt ’93. This attack is based on finding linear approximations to describe the transformations performed in DES (and other block ciphers). This method can find a DES key given 247 known plaintexts, as compared to 247 chosen plaintexts for differential cryptanalysis (it is therefore a known plaintext attack although it can also work as a ciphertext only attack). Although this is a minor improvement (because it may be easier to acquire known plaintext rather than chosen plaintext) it still leaves linear cryptanalysis infeasible as an attack on DES. However it is useful for an understanding of other similar attacks and gives an insight into why the S-boxes are constructed the way they are.

Birthday attack

The Birthday attack makes use of what’s known as the Birthday paradox to try to attack cryptographic hash functions. The birthday paradox can be stated as follows: What is the minimum value of k such that the probability is greater than 0.5 that at least two people in a group of k people have the same birthday? It turns out that the answer is 23 which is quite a surprising result. In other words if there are 23 people in a room, the probability that two of them have the same birthday is approximately 0.5. If there is 100 people (i.e. k=100) then the probability is .9999997, i.e. you are almost guaranteed that there will be a duplicate. A graph of the probabilities against the value of k is shown in Figure 3

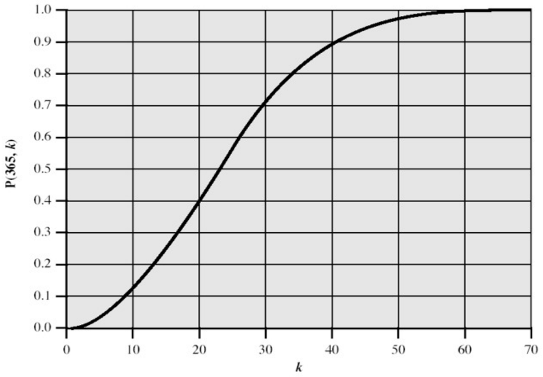

Figure 3 : Birthday attack

Implementation Attacks

Implementation attacks take on a different approach to the above for discovering the secret key. Instead of attacking the mathematical properties of the algorithm these form of attacks (also known as side channel attacks) take advantage of the physical phenomena that occurs when a cryptographic algorithm is implemented in hardware. Four side channel attacks are listed in the FIPS standard 140-2 “Security Requirements for Cryptographic Modules”, **Power Analysis**, **Timing Analysis**, **Fault Induction** and **TEMPEST**.

1. **Power Analysis:** Attacks based on the analysis of power consumption can be divided into two categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are obtained through monitoring the variations in electrical power consumption of a cryptographic module for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently values of cryptographic keys. DPA has the same goals but utilizes advanced statistical methods and/or other techniques to analyze the variations of the electrical power consumption of a cryptographic module. Cryptographic modules that utilize external power (direct current) sources appear to be at greatest risk. Methods that may reduce the overall risk of Power Analysis attacks include the use of capacitors to level the power consumption, the use of internal power sources, and
the manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing.

2. **Timing Analysis:** Timing Analysis attacks rely on precisely measuring the time required by a cryptographic module to perform specific mathematical operations associated with a cryptographic algorithm or process. The timing information collected is analyzed to determine the relationship between the inputs to the module and the cryptographic keys used by the underlying algorithms or processes. The analysis of the relationship may be used to exploit the timing measurements to reveal the cryptographic key or CSPs (Cryptographic Security Parameters). Timing Analysis attacks assume that the attacker has knowledge of the design of the cryptographic module. Manipulation of the individual operations of the algorithms or processes to reduce timing fluctuations during processing is one method to reduce the risk of this attack.

3. Fault Induction: Fault Induction attacks utilize external forces such as microwaves, temperature extremes, and voltage manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns can be used in an attempt to reverse engineer the cryptographic module, revealing certain features and implementations of cryptographic algorithms and subsequently revealing the values of cryptographic keys. Cryptographic modules with limited physical security appear to be at greatest risk. Proper selection of physical security features may be used to reduce the risk of this attack.

4. **TEMPEST:** TEMPEST attacks involve the remote or external detection and collection of the electromagnetic signals emitted from a cryptographic module and associated equipment during processing. Such an attack can be used to obtain keystroke information, messages displayed on a video screen, and other forms of critical security information (e.g., cryptographic keys). Special shielding of all components, including network cabling, is the mechanism used to reduce the risk of such an attack. Shielding reduces and, in some cases, prevents the emission of electromagnetic signals. If a cryptographic module is designed to mitigate one or more specific attacks, then the modules security policy shall specify the security mechanisms employed by the module to mitigate the attack(s). The existence and proper functioning of the security mechanisms will be validated when requirements and associated tests are developed.

IV. DEFENDING ATTACKS ON CRYPTOSYSTEMS

Creating effective cryptographic systems requires balancing business protection needs with technical constraints. It is critical that these technologies be included as part of an effective and holistic protection solution. It is not enough to simply implement encryption and assume all risks have been addressed. For example, just because an e-mail system is using message encryption, it does not necessarily mean that e-mail is secure, or even any better than plaintext. When considering a protection system, not only must one look at and test the underlying processes, but one must also look for ways around the solutions and address these risks appropriately. It is vital to understand that crypto solutions can be dangerous because they can easily lead to a false sense of information security.

Design, Analysis, and Testing

Fundamental to the successful implementation of a cryptosystem are thorough design, analysis, and testing methodologies. The implementation cryptography is probably one of the most difficult and most poorly understood IT fields. Information technology and security professionals must fully understand that cryptographic solutions that are

DOI10.17148/IJARCCE.2017.6570

simply dropped into place are doomed to failure. It is generally recommended that proprietary cryptographic systems are problematic and usually end up being not quite what they appear to be. The best algorithms are those that have undergone rigorous public scrutiny by crypto experts. Just because a cryptographer cannot break his or her own algorithm, this does not mean that this is a safe algorithm. As Bruce Schneier points out in "Security Pitfalls in Cryptography," the output from a poor cryptographic system is very difficult to differentiate from a good one. Smith13 suggests that preferred crypto algorithms should have the following properties:

- No reliance on algorithm secrecy
- Explicitly designed for encryption
- Available for analysis
- Subject to analysis
- No practical weaknesses

When designing systems that use cryptography, it is also important to build in proper redundancies and compensating controls, because it is entirely possible that the algorithms or implementation may fail at some point in the future or at the hands of a determined attacker.

Selecting Appropriate Key Lengths Although proper design, algorithm selection, and implementation are critical factors for a cryptosystem, the selection of key lengths is also very important. Security professionals and their IT peers often associate the number of "bits" a product uses with the measure of its level of protection. In theory, the greater the key length, the more difficult the encryption is to break. However, in practice, there are performance and practical concerns that limit the key lengths to be used. In general, the following factors will determine what key sizes are used:

- Value of the asset it is protecting (compare to cost to break it)
- Length of time it needs protecting (minutes, hours, years, centuries)
- Determination of attacker (individual, corporate, government)
- Performance criteria (seconds versus minutes to encrypt/decrypt)

Random Number Generators

As discussed earlier, random number generators are critical to effective cryptosystems. Hardware-based RNG are generally believed to be the best, but more costly form of implementation. These devices are generally based on random physical events, and therefore should generate data that is nearly impossible to predict. Software RNGs obviously require additional operating system protection, but also protection from covert channel analysis.

V. CONCLUSION

The appropriate use of cryptography is critical to modern information security, but it has been shown that even the best defenses can fail. It is critical to understand that cryptography, while providing excellent protection, can also lead to serious problems if the whole system is not considered. Eventually, experts must understand not only the details of the crypto products they are using, but what they are in fact protecting, why these controls are necessary, and who they are protecting these assets against.

REFERENCES

[1] Behrouz A Forouzan, "Data Communications and networking", McGraw-Hill, 4th Edition.
[2] Gary C. Kessler, An overview of Cryptography, 28April2013 http://www.garykessler.ne/library/crypto.html
[3] RSA Laboratories- Cryptographic tools; section 2.1.5. Unpublished: http://www.rsa.com/rsalabs/node.asp?id=217
[4] Ing. Cristian MARINESCU, prof.dr.ing. Nicolae ŢĂPUŞ ; "An Overview of the Attack Methods Directed Against the RSA Algorithm"; Revista Informatica Economica, nr. 2(30)/2004
[5] Stallings, W.: Cryptography and Network Security, Prentice Hall, (2010).
[6] Matsui M. (1994) Linear Cryptanalysis Method for DES Cipher. In: Helleseth T. (eds) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993.
[7] Information security Management Handbook Chapter 94
[8] D.Boneh,R.DeMilo and R.lipton.On the importance of checking cryptographic protocols for faults.In EUROCRYPT'97,Volume 1233 of Lecture Notes in omputer Science,Pages 37-51,Springer,verilag 1997
[9] A.Menezes,P.Van Oorschot and S.Vanstone Handbook og applies cryptography CRC,1996

DOI10.17148/IJARCCE.2017.6570