International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.82.031

Comparison of White Box, Black Box and Gray Box Cryptography

Jasleen Bhatia
CSE Department, GTBIT, GGSIPU
New Delhi, India

Abstract- This paper is focused on a study of security issues related to an execution of cryptographic algorithms in an untrusted environment. It is therefore clear that algorithms built for both Black and Gray box models are impractical in the face of operating on non-trusted hosts. Understandably, hackers will not try to break the cipher by only using the means available in Black and Gray box scenarios, instead they will observe the execution when the unprotected key is used – directly stealing it.The word cryptology is derived from the Greek words krypt´os, meaning 'hidden', and logos, meaning 'word'. Strictly speaking, it is the science that studies how to hide confidential information. Cryptology comprises of two complementary fields. Cryptography is the study and practice of hiding information, while cryptanalysis is the study of methods to obtain knowledge from hidden information.

Keywords-Attacks in White Box Cryptography, Black Box Model, Gray Box Model, White Box Model.

I. INTRODUCTION

Attack contexts for cryptography module can be classified as black box, gray box, and white box attacks. Among which white box attack is considered to be the strongest attack and the adversary has all the privileges and also has complete access to the implementation of the algorithm and its dynamic execution.

White box cryptography prevents key extraction by using one of its methods to hide the key in lookup tables. The adversary cannot find the secret key in physical memory as it cannot be seen in the memory directly. Thus white box cryptography is used to provide high security. The performance is affected due to the large size of the lookup table and the encoding and decoding process.[1]

White box cryptography is the new technique against attacks on white box attack environments. In white box attack model, the attacker is even stronger than in black box attack model, and the attacker can monitor all intermediate values.

Therefore, safety algorithms are needed against all operation steps being exposure. In white box attack, an attacker has full access to the software implementation of a cryptographic algorithm where the binary is completely visible and alterable by the attacker and the attacker has full control over the execution platform (CPU calls, memory registers, etc.)

1.1 ORGANIZATION

Introduction in this paper is starting with attack contexts for cryptography module can be classified as black box, gray box, and white box attacks. . Among which white box attack is considered to be the strongest attack and the adversary has all the privileges and also has complete access to the implementation of the algorithm and its dynamic execution.

It is concluded that white-box cryptography is more appropriate than black-box and gray-box cryptography. Security of a cryptographic algorithm is studied in the "black-box" model: e.g., for symmetric encryption, the attacker is given access to a "device" which runs the encryption algorithm with a given key. In the "gray-box" model, the attacker also has access to some partial side-channel information; this is where power analysis fits. In the "white-box" model, the attacker has full access to the internal state. The white-box model is meant for: "the algorithm runs as software on the attacker's own computer".

II. ATTACKS IN WHITE BOX CRYPTOGRAPHY

There are three types of attacks toward cryptographic module - Black-box attack, Gray-box attack and white-box attack.[2]

- *Black-box attack*

- Watches inputs and outputs
- Controls input text
- No visibility of execution

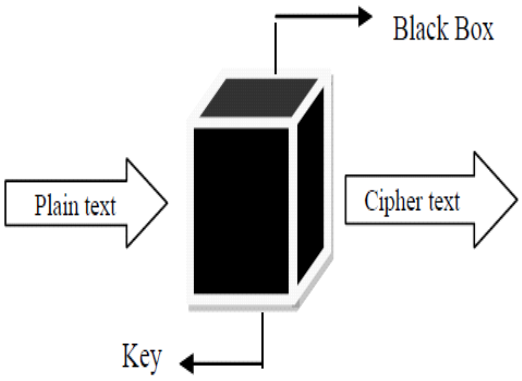

Figure 2.1.1: Black Box Attack

Gray Box Attack

- The Gray box scenario assumes that the attacker has partial physical access to the Key or that it is "leaking" so called side channel information.
- Side Channel Analysis attacks (SCA) exploit information leaked from the physical implementation of a cryptographic system.
- The leakage is passively observed via timing information, power consumption, and electromagnetic radiations.[2]

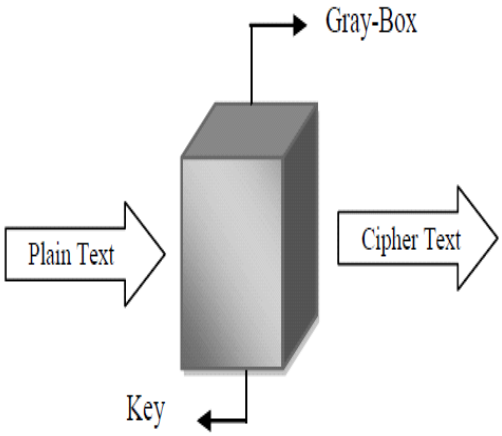

Figure2.1. 2: Gray Box Attack

2.3 White-box attack

- Attacker can observe everything.
- Attacker knows algorithm.
- Watches inputs, outputs, and intermediate calculations.
- Controls input text.
- Full visibility into Memory (debuggers and emulators).

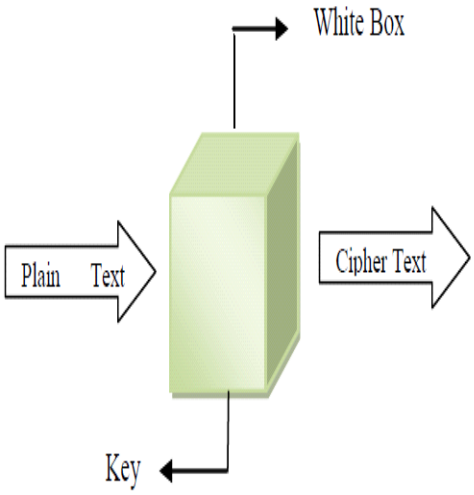

Figure 2.1.3: White Box Attacks

III. MODELS

3.1 BLACK BOX MODEL

This module assumes that the attacker has no physical access to the key or internal workings, but can only observe the external information and behaviour. The information consist of either revealing the plaintext or the cipher text of the system assuming zero visibility on code execution and dynamic encryption operations.
There are three levels of attacks in the black box model. The first being passive attack which is also known as the plaintext attack which can only observe the input and output of the black box system. The second one being active attack which is also known as plain text attack which involves direct interaction.[3] The third attack is the adaptive attack known as the plaintext-ciphertext attack. This attack gathers information by choosing a ciphertext and obtains its decryption using an unknown key. This attack may lead to knowing the ciphertext and obtaining the resulting plaintext.
The Black box scenario, being a traditional model, assumes that the attacker has no physical access to the Key (algorithm performing the encryption or decryption) or any internal workings, rather can only observe external information and behavior. This information consists of either the plaintext (input) or the ciphertext (output) of the system while assuming zero visibility on code execution and dynamic encryption operations.[11]

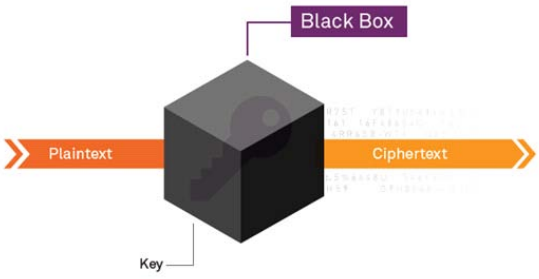

Figure 3.1.1: Black Box Cryptography

3.2 GRAY BOX MODEL

The gray box model is also known as the side channel attack or the partial access attack. The attacks are based on information gained from physical implementation of cryptosystem rather than a brute force attack. The adversary gains information from power consumption, timing, fault analysis and uses the information to break the system. The gray box attack states that any visibility to the inner working, side effect or execution of an algorithm can weaken the security.

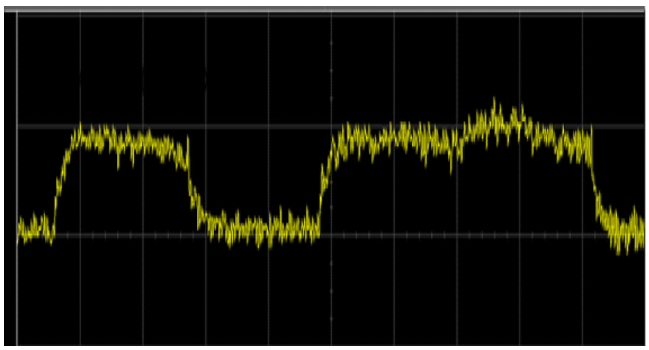

Figure 3.2.1: Power Analyser of RSA key bits

In the above example we can see an attempt made to decode RSA key bits using power analysis. The left peak represents the CPU power variations during the step of the algorithm without multiplication; the right peak shows a step with multiplication, allowing to read bits 0, 1.[5]
The Gray box scenario assumes that the attacker has partial physical access to the Key or that it is "leaking" so called side channel information. Side Channel Analysis attacks (SCA) exploit information leaked from the physical implementation of a cryptographic system. The leakage is passively observed via timing information, power consumption, electromagnetic radiations, etc. Protection against Side Channel Attacks is important because the attacks can be implemented quickly and at a low cost. Publicly available side channel information allows hackers to effectively reveal parts of the Key and as a result dramatically reduce its efficacy and demote the overall protection.[3]

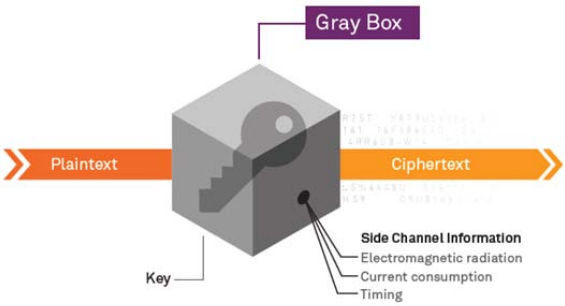

Figure 3.2.2: Gray Box Cryptography

3.3 WHITE BOX MODEL

In this model the adversary has full control of the targets execution environment assuming that:
- Attacks with full privilege have complete access to the implementation algorithms.
- Dynamic execution can be observed and important data such as cryptographic keys can be seen.
- Detailed algorithms in the system are completely visible and alterable.

The adversary extracts the cryptographic key in this model as he knows all the algorithms and observes the dynamic execution, through which he can extract the keys from the memory. The adversary using this type of model attack

has the strongest power to the cryptography system. To protect them techniques like obfuscation and temper resistance is used.

The White box scenario, in contrast with previously described scenarios, handles far more severe threats while assuming hackers have full visibility and control over the whole operation. Hackers can freely observe dynamic code execution (with instantiated cryptographic keys) and internal algorithm details are completely visible and alterable at will. Despite this fully transparent methodology, White box cryptography integrates the cipher in a way that does not reveal the key.

It is therefore clear that algorithms built for both Black and Gray box models are impractical in the face of operating on non-trusted hosts. Understandably, hackers will not try to break the cipher by only using the means available in Black and Gray box scenarios, instead they will observe the execution when the unprotected key is used – directly stealing it.

Traditional cryptography algorithms, as exposed in the White box scenario, assume the presence of the key as part of the implementation.

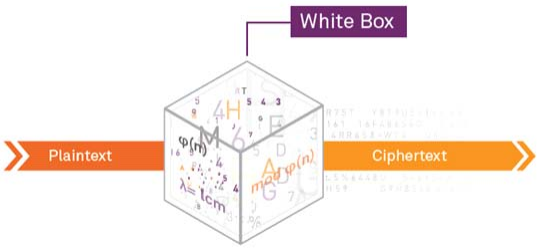

Figure 3.3.1: White Box Cryptography

The White box cryptography algorithm is protected in the White box scenario, as the key is not present in memory and cannot be extracted – not even dynamically.[11]

Choosing the most appropriate, most secure cryptographic model is therefore the sole line of defense against malicious threats – precisely what White box cryptography attempts to achieve.

IV.CONCLUSIONS

It is found that white-box cryptography is more appropriate than black-box and gray-box cryptography. Security of a cryptographic algorithm is studied in the "black-box" model: e.g., for symmetric encryption, the attacker is given access to a "device" which runs the encryption algorithm with a given key. In the "gray-box" model, the attacker also has access to some partial side-channel information; this is where power analysis fits. In the "white-box" model, the attacker has full access to the internal state. The white-box model is meant for: "the algorithm runs as software on the attacker's own computer".

REFERENCES

[1] Brecht Wyseur, "White-Box Cryptography," PhD thesis, Katholieke Universiteit Leuven, Bart Preneel
[2] A. Saxena, Brecht Wyseur, and Bart. Preneel, "Towards Security Notions for White-Box Cryptography"
[3] S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot , 16 August 2002,"White-Box Cryptography and an AES Implementation", (SAC'02), Ottawa, Canada.
[4] Marjanne Plasmans ,2005.,"White-Box Cryptography for Digital Content protection", department of mathematics and computer science
[5] http://link.springer.com/chapter/10.1007/3-540-36492-7_17
[6] http://www.whiteboxcrypto.com/
[7] http://www.whiteboxcrypto.com/files/phdPresentation.pdf.
[8] http://developeriq.in/articles/2013/sep/26/understanding-white-box-cryptography/