A Closer Look at Attacks on Lightweight Cryptosystems: Threats and Countermeasures

Khusanboy Kodirov, Hoon-Jae Lee, and Young Sil Lee(✉)

Computer Engineering, Dongseo University, Busan 47011, Korea
hjlee@gdsu.dongseo.ac.krs, lys0113@dongseo.ac.kr

Abstract. Cryptosystems are fundamental to securing digital communication and information exchange in our interconnected world. However, as technology advances, so does the sophistication of malicious actors seeking to compromise these cryptographic mechanisms. A branch of cryptosystems called lightweight cryptography plays a pivotal role in ensuring secure communication and data protection in resource-constrained devices, such as IoT sensors and embedded systems. This paper provides an in-depth exploration of the attack vectors that lightweight cryptosystems face and introduces novel technical countermeasures aimed at bolstering their security. The research in this paper is positioned at the forefront of lightweight cryptography, aiming to address current and emerging threats.

Keywords: Cryptosystems · Cryptanalysis · Lightweight Encryption · Attacks

1 Introduction

From the ages, human beings had two inherent needs. First, to communicate and share information, and second, to communicate selectively. These two needs led people to create the art of coding the messages so that only authorized and intended personnel could access the information. Even if the scrambled secret messages fell into the hands of unintended people, they could not decipher the message and extract any hidden information. During 500 to 600 BC, Romans used a mono-alphabetic substitution cipher known as Caesar Shift Cipher which relied on shifting the letters of a message by some agreed amount (Fig. 1).

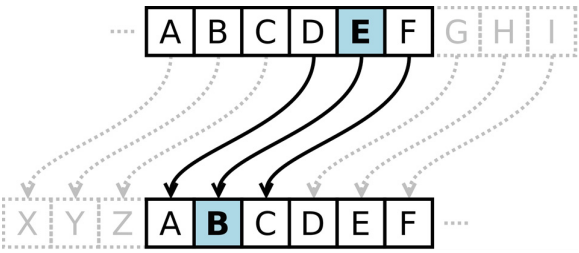

Fig. 1. Caesar Shift Cipher

B. J. Choi et al. (Eds.): IHCI 2023, LNCS 14532, pp. 171–176, 2024.
https://doi.org/10.1007/978-3-031-53830-8_17

In the 20th and 21st centuries, many encryption standards have been developed by computer scientists and mathematicians. Nowadays, in almost every aspect of human life, there is a need to transfer information secretly. As a result, it has become essential to protect useful information from cyber-attacks. This paper discusses some of the most common attacks on cryptosystems by each category and the necessary countermeasures to ensure the information being communicated is as secure as possible.

1.1 Lightweight Cryptography

Lightweight cryptography plays a pivotal role in ensuring secure communication and data protection in resource-constrained devices, such as IoT sensors and embedded systems. This paper provides an in-depth exploration of the attack vectors that lightweight cryptosystems face and introduces novel technical countermeasures aimed at bolstering their security. The research in this paper is positioned at the forefront of lightweight cryptography, aiming to address current and emerging threats.

2 Related Work

A significant amount of related work has been conducted in the field of securing lightweight encryption. Researchers have focused on various aspects of lightweight encryption, including threat analysis, vulnerabilities, and countermeasures. Here are some key areas of related work:

2.1 Side-Channel Analysis and Countermeasures:

There is a substantial body of research on side-channel attacks against lightweight encryption algorithms. Countermeasures like masking, blinding, and secure implementations have been proposed to mitigate these attacks (Fig. 2).

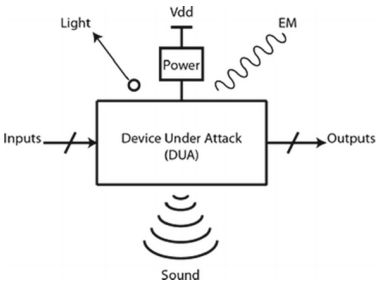

Fig. 2. Side channel attack

Frequently employed side-channel inputs encompass elements like power supply voltage, temperature, ambient light, and other primary signals not directly associated with the cryptographic module. These attacks involve a combination of monitoring side-channel outputs, manipulating side-channel inputs, observing primary outputs, and

tampering with primary inputs. These activities are accompanied by progressively intricate analytical methods aimed at uncovering confidential data from the cryptographic system.

2.2 Light Lightweight Cryptographic Algorithm Design:

Researchers have developed and analyzed lightweight cryptographic algorithms designed specifically for resource-constrained devices. These algorithms aim to strike a balance between security and efficiency.

3 Types of Attacks on Cryptosystems

3.1 Passive Attacks

In order to obtain unauthorized access to the information, a passive attack is carried out. For instance, when an attacker intercepts or eavesdrops on the communication channel, it is regarded as a passive attack (Fig. 3).

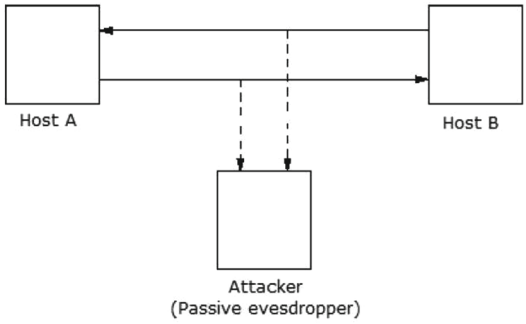

Fig. 3. Passive Attack

It is called a passive attack in nature since the attacker neither affects the information being transferred nor disrupts the communication channel. It can be seen as stealing information. As information theft may go unnoticed by the owner, this type of attack can be more dangerous.

3.2 Active Attacks

Contrary to a passive attack, an active attack involves altering the information in some way by conducting a certain process on the data (Fig. 4).

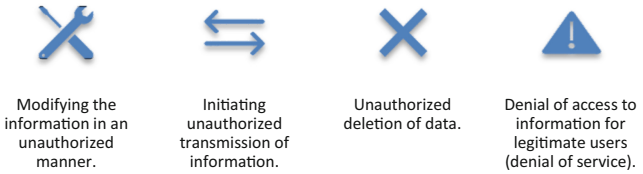

Fig. 4. Active Attack

4 Cryptographic Attacks

The main intention of an attacker is usually to break a cryptosystem and extract the plaintext from the ciphertext. As for the symmetric key encryption, the attacker only needs the secret key to obtain the plaintext, as in most cases, the algorithm itself is already in the public domain. For this, he (or she) takes maximum effort to find the secret key used in that particular communication channel. A cryptosystem is considered broken or compromised once the attacker successfully obtains the secret encryption key. Let us look at some of the most common attacks carried out on cryptosystems by each category .

4.1 Ciphertext Only Attacks (COA)

It involves a scenario where the attacker possesses a collection of ciphertexts but lacks access to their corresponding plaintexts. Success in COA is achieved when one can deduce the corresponding plaintext from the provided ciphertext set. In some cases, this type of attack may even reveal the encryption key. It's worth noting that contemporary cryptosystems are designed with robust defenses against ciphertext-only attacks to enhance security.

4.2 Known Plaintext Attack (KPA)

In this approach, the attacker possesses knowledge of the plaintext for certain portions of the ciphertext. The objective is to decipher the remaining ciphertext with the assistance of this known information. Achieving this can involve techniques such as identifying the encryption key or employing alternative methods. A prominent illustration of such an attack is seen in linear cryptanalysis when applied to block ciphers.

4.3 Dictionary Attack

This type of attack comes in various forms, but they all revolve around creating a 'dictionary.' In its most straightforward form, the attacker constructs a dictionary containing pairs of ciphertexts and their associated plaintexts that they have gathered over time. When faced with ciphertext in the future, the attacker consults this dictionary to identify the corresponding plaintext.

4.4 Brute Force Attack (BFA)

In this approach, the attacker ascertains the key by systematically testing every conceivable key. For instance, if the key consists of 8 bits, there are a total of 256 possible keys (2^8 = 256). Armed with knowledge of the ciphertext and the encryption algorithm, the attacker proceeds to test all 256 keys individually in an attempt to decrypt the data. However, if the key is lengthy, this method would require significant time to complete the attack due to the sheer number of potential keys (Fig. 5).

4.5 Man in Middle Attack (MIM)

This attack primarily focuses on public key cryptosystems that employ a key exchange process prior to initiating communication.

- Host A seeks to establish communication with host B and, consequently, requests the public key belonging to B.
- However, an assailant intercepts this request and substitutes their own public key.
- As a result, anything that host A transmits to host B becomes accessible to the attacker.
- To sustain the communication, the attacker re-encrypts the data with their public key after intercepting and reading it and then forwards it to B.
- The attacker disguises their public key as if it were A's public key, causing B to accept it as if it were originating from A.

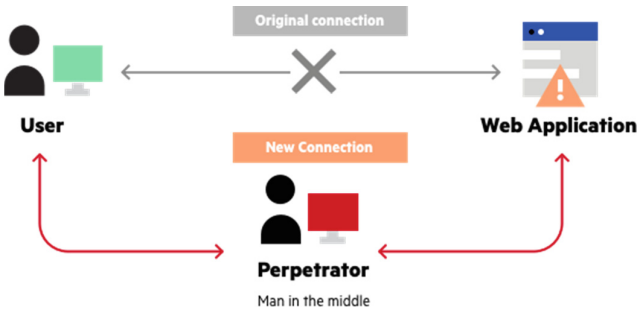

Fig. 5. Man in Middle Attack (MIM)

5 Countermeasures for Lightweight Encryption

5.1 Fault Injection Attacks and Protections:

Lightweight devices are vulnerable to fault injection attacks. Researchers have investigated fault attacks and proposed methods to protect lightweight cryptographic algorithms, such as error-detection codes and fault tolerance techniques.

5.2 Post-quantum Lightweight Cryptography:

With the advent of quantum computing, researchers are exploring lightweight cryptographic primitives that can resist quantum attacks. This includes lattice-based and code-based cryptography suitable for resource-constrained devices.

5.3 Energy-Efficient Cryptography:

Energy-efficient cryptographic algorithms are developed for low-power devices, considering the unique constraints of these systems. This work focuses on achieving security while minimizing energy consumption.

5.4 Machine Learning and Lightweight Cryptography:

Recent research has explored the application of machine learning techniques to enhance the security of lightweight cryptographic algorithms by identifying patterns and anomalies in data.

6 Conclusion

In conclusion, the world of cryptosystems is one where innovation and security continually collide with evolving threats. The paper concludes by summarizing the key findings and emphasizing the importance of addressing threats to lightweight cryptosystems with innovative countermeasures. The research presented in this paper is a testament to the ongoing development of lightweight cryptography, ensuring the security and privacy of resource-constrained devices. However, as the landscape of cyber threats continues to evolve, so too do the countermeasures and defense mechanisms designed to sfight against these attacks. The arsenal of countermeasures is diverse and dynamic, from employing state-of-the-art encryption algorithms and key management practices to fostering a culture of security awareness and regulatory compliance.

Acknowledgment. This research was supported by Korea Institute of Marine Science & Technology Promotion (KIMST) funded by the Ministry of Oceans and Fisheries (20210650).

References

1. Smith, J.: Attacks on cryptosystems: vulnerabilities and countermeasures. Int. J. Cybersecurity **12**(3), 401–420 (2023)
2. Johnson, A.L.: Cryptanalysis techniques and their role in cryptosystem security. J. Inf. Secur. Res. **7**(1), 56–72 (2023)
3. Brown, E.R., Garcia, M.P.: Enhancing cryptosystem resilience: a comprehensive review of countermeasures. Cybersecurity J. **15**(2), 189–210 (2023)
4. Chen, Q., Kim, S.H.: Social engineering attacks on cryptosystems: strategies and mitigation. J. Comput. Secur. **25**(4), 509–528 (2023)
5. Williams, R.T., Lee, C.H.: Quantum threats to cryptosystems: challenges and defenses. Cryptology Today **9**(4), 315–333 (2023)