

KLEPTOGRAPHY: THE HIDDEN THREAT IN CRYPTOGRAPHIC SYSTEMS

Вінницький національний технічний університет

Анотація

У тезах розглянуто поняття клептографії як методу прихованого витікання секретної інформації через криптографічні системи. Проаналізовано основні методи реалізації бекдорів, їхній вплив на безпеку користувачів і компаній, а також можливості використання різними суб'єктами. Особливу увагу приділено методам запобігання клептографічним атакам, зокрема перевірці відкритого коду, використанню надійних генераторів випадкових чисел та незалежному аудиту криптографічних систем.

Ключові слова: клептографія, криптографія, стеганографія, бекдор, безпека, витік даних, криптографічний аудит, генератори випадкових чисел.

Abstract

The theses consider the concept of kleptography as a method of covert leakage of secret information through cryptographic systems. The main methods of implementing backdoors, their impact on the security of users and companies, as well as the possibilities of use by various entities are analyzed. Special attention is paid to methods of preventing kleptographic attacks, in particular, checking open source code, using reliable random number generators, and independent auditing of cryptographic systems.

Keywords: kleptography, cryptography, backdoor, security, data leakage, cryptographic audit, random number generators.

In today's digital world, cryptography plays a key role in protecting information, ensuring confidentiality, integrity, and authentication of data. However, alongside traditional threats such as cryptanalysis or attacks on weak algorithms, there is a less obvious but no less dangerous threat – kleptography.

Kleptography is an approach that involves using cryptographic algorithms with hidden vulnerabilities that allow attackers to extract confidential information, such as secret keys. These vulnerabilities can be intentionally built into software, hardware, or encryption standards, creating backdoors that are difficult to detect.

Relevance of the problem: Given that cryptography is used in banking systems, online communications, digital signatures, and secure data storage, the implementation of kleptographic mechanisms can have catastrophic consequences. Even if the system appears secure, hidden backdoors allow attackers to access protected data without the knowledge of the users. This problem is especially acute in cases where cryptographic mechanisms are developed or supported by government agencies or private corporations with opaque interests.

One of the main threats of kleptography is the covert leakage of secret keys through intentionally modified cryptographic algorithms. Such attacks can be built into the encryption algorithm during its design or implementation in software or hardware. The main mechanism of leakage [1] is based on the creation of a backdoor that allows an attacker to obtain secret data without explicitly interfering with the encryption process. For example, the ciphertext may contain hidden clues about the secret key, or the malicious code may exploit weaknesses in the random number generator to make the key predictable.

Kleptography, cryptography, and steganography [2] have a common connection with information security, but they perform fundamentally different tasks. Cryptography focuses on protecting data from unauthorized access by transforming it using encryption, ensuring confidentiality, integrity, and authentication. Steganography, unlike cryptography, does not change the content of the message, but hides the very fact of its existence by embedding data in digital media, such as images or audio files. Kleptography, on the other hand, has a malicious purpose and is used to covertly leak secret information, in particular encryption keys, by introducing invisible backdoors into cryptographic algorithms. This allows an attacker to gain access to encrypted data without the knowledge of users using the compromised system. Thus, if cryptography protects information, and steganography hides its transmission, then kleptography, on the contrary, creates a security threat, acting covertly within the cryptographic mechanisms themselves.

Backdoors in cryptographic systems are hidden mechanisms that allow attackers to gain access to encrypted data or secret keys without the knowledge of the user or system administrator [2]. They can be built into various stages of the cryptographic process, including encryption algorithms. For example, one method of implementing a backdoor is to modify a cryptographic algorithm in such a way that certain individuals or processes can decrypt data without the knowledge of the legitimate user. This can be achieved by introducing "weak spots" into the algorithm structure itself or by creating additional invisible keys for decryption.

Another way to implement a backdoor is to have secret keys that are hidden in the system and known only to the developers or third parties implementing malicious access. Such keys can be embedded in the program code or configuration files of the system, allowing access to encrypted data without having to go through standard authentication mechanisms. In the case of the use of malicious certificates and digital signatures, it is possible to create a situation where the data appears legitimate, but is actually part of a malicious access scheme.

Another method of implementing a backdoor is to use systems with limited access controls, where administrators or certain users can bypass standard security mechanisms. This can include the creation of backup or "black" accounts that allow attackers to access data without the knowledge of the main users [3]. Finally, steganography, which is often used in conjunction with encryption, can also be a tool for implementing a backdoor. In this case, the information that allows attackers to access encrypted files may be hidden within the files themselves or in data transfer processes.

Kleptography, as a tool for covertly leaking information from cryptographic systems, poses serious potential security risks to users and companies. Since cryptography is widely used to protect sensitive data such as financial information, personal data, and corporate secrets, the introduction of covert access channels can lead to the leakage of this information. Attackers, having gained access to such systems, can steal critical data or even manipulate it, which poses a danger to corporate structures, banks, governments, and even individuals. In particular, businesses can suffer serious financial losses, loss of reputation, or even legal consequences due to the theft of customer data or violation of contract terms.

In addition, the impact of kleptography on the trust in cryptographic technologies is significant. If users or companies learn that there are hidden opportunities for unauthorized access to their encrypted data, this can undermine their trust in the very principles of information protection. Cryptographic technologies that are designed to ensure confidentiality and integrity of data can be lost due to the introduction of such hidden access channels. This can lead to a decline in the popularity of cryptography in such critical areas as online banking, e-commerce and the transfer of confidential information in government agencies [1].

The use of kleptography by state agencies or attackers also has serious consequences. In the case where states use kleptography to gain access to information, this can lead to violations of citizens' rights to privacy and personal freedoms. Some governments can use such technologies to spy on or monitor their own citizens, which has drawn global criticism from human rights organizations. Attackers, in turn, can use kleptography to prepare cyberattacks, gather intelligence, or conduct other illegal operations. In both cases, kleptography can be used to adjust the balance of power in favor of those who have access to the hidden

capabilities of these systems, which requires increased international control and regulation of cryptographic technologies.

Open source and cryptographic standards verification are important steps in ensuring the security of cryptographic systems. Since open source allows third-party researchers to study, test, and improve software, it is one of the main ways to identify vulnerabilities in systems. In addition, the use of cryptographic standards such as AES, RSA, and others ensures that systems operate according to best practices and recommendations from international organizations. Open source and standards allow independent experts to verify that the correct algorithms are being used and that the system does not contain hidden vulnerabilities or unwanted mechanisms such as backdoors or kludges.

The use of deterministic random number generators (DRNGs) is a critical aspect of cryptography, as many algorithms rely on the generation of random numbers to generate keys, initialization vectors, or other important elements. Unreliable or poor-quality random number generators can lead to vulnerabilities that allow attackers to predict or recover secret keys. Deterministic random number generators, which always generate the same sequence of numbers from the same seed, should be avoided as this reduces security. To ensure high reliability of cryptographic systems, it is recommended to use randomness sources that are based on physical processes or complex mathematical algorithms that cannot be predicted [4].

Auditing cryptographic systems and independent verifications are critical to ensuring confidence in the security system. Audits allow you to verify whether cryptographic algorithms have been properly implemented and whether they do not contain vulnerabilities that can be exploited for hacking. Independent verifications conducted by third-party experts or organizations help ensure objectivity and reduce the risk of bias in the development of cryptographic mechanisms. Such verifications may include penetration testing, checking the code for backdoors, and assessing compliance with international security standards, which ensures that cryptographic systems are reliable and resistant to attacks.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. МЕТОДИ ЗАХИСТУ БАНКІВСЬКОЇ ІНФОРМАЦІЇ.
URL: http://dspace.wunu.edu.ua/bitstream/316497/574/1/metodu_zah_bank_inf.pdf (date of access: 01.03.2025).
2. КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ.
URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34907/90812.pdf?sequence=2&isAllowed=y> (date of access: 01.03.2025).
3. Kleptography: Using Cryptography Against Cryptography.
URL: https://www.researchgate.net/publication/221348188_Kleptography_Using_Cryptography_Against_Cryptography (date of access: 01.03.2025).
4. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ.
URL: <https://files.znu.edu.ua/files/Bibliobooks/Inshi78/0058486.pdf> (date of access: 01.03.2025).

Іванова Людмила Євгенівна – студентка групи ІБКС-23б, факультет інформаційних технології та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: milaivanova2609@gmail.com

Дерун Віталіна Гарольдівна – старший викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: derun@vntu.edu.ua

Ivanova Liudmila Yevheniivna – student of group 1BKS-23b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: milaivanova2609@gmail.com

Derun Vitalina Haroldivna – Senior Lecturer, Department of Foreign Languages, Vinnytsia National Technical University, Vinnytsia, e-mail: derun@vntu.edu.ua