Intrusions into Cryptographic Systems and Their Digital Forensic Analysis

Orkhan Valikhanli
Institute of Information Technology, Baku, Azerbaijan
orkhanvalikhanli@gmail.com

***Abstract*— Cryptographic systems are important for protecting information. They are used to secure data, ensure privacy, and authenticate users in various fields, including communication, online banking, government services, etc. Despite their strong security capabilities, these systems remain vulnerable to cyberattacks. In most cases, cryptographic algorithms are not attacked directly. Instead, vulnerabilities in the system's implementation, architecture, and key management are exploited. This study examines intrusions into cryptographic systems and investigates the corresponding digital forensic aspects.**

Keywords*— *cryptographic system; attack; digital forensic analysis; forensic tools; intrusion;

I. INTRODUCTİON

A cryptographic system is a set of cryptographic algorithms, methods, and protocols used to protect information. A cryptographic system defines a set of requirements for the selection of cryptographic algorithms and their parameters, as well as the rules for the generation, transmission, processing, and storage of key information [1].

Cryptographic systems play an important role in numerous application domains. For online banking, protect user credentials and secure financial transactions. In modern communication systems, encryption protects messages, emails, images, videos, etc., from various types of cyberattacks. For government services, citizen data and confidential communications are protected using digital signatures, encryption, and secure identification methods. In e-commerce, encryption protects online purchases, user accounts, and data exchange. For cloud storage, various cryptographic mechanisms are used to secure stored information, services, and file sharing. In healthcare systems, cryptographic methods are used to protect medical transactions and records.

Cryptographic systems are designed to ensure the confidentiality, integrity, and authenticity of information. However, they remain vulnerable to intrusions. Attackers may use various techniques against cryptographic systems. Although the cryptographic algorithm itself is generally safe, weak passwords, improper key management, and system configuration flaws can lead to serious incidents.

Digital forensics plays an important role in investigating these incidents. It involves various steps to determine how an intrusion took place and what information was affected. In cryptographic system intrusions, forensic investigators examine system logs, encrypted files, digital certificate files, volatile memory, network traffic, and other important evidence for investigation. This enables investigators to identify attackers and understand their attack techniques. The findings are also used to improve system security and protect against future attacks.

This study examines intrusions into cryptographic systems and also discusses their digital forensic aspects. The paper is organized as follows. In Section II, intrusion into cryptographic systems is discussed. In Section III, digital forensic analysis of cryptographic systems is presented. In Section IV, security measures for cryptographic systems are discussed. Section V presents the conclusion of this study.

II. INTRUSIONS INTO CRYPTOGRAPHIC SYSTEMS

Intrusions into cryptographic systems can be defined as unauthorized actions or attempts that target the confidentiality or integrity of cryptographic mechanisms. There are various types of attacks that target cryptographic systems. These include cryptanalysis, brute-force, side-channel attack, and man-in-the-middle (MITM).

A. Cryptanalysis attacks

Cryptanalysis is the set of techniques used to uncover secret information from encrypted data (ciphertext) [2]. There are several cryptanalysis techniques as presented below:

- Known-plaintext attack – both the plaintext and the corresponding ciphertext are accessible to an attacker. The goal is to use the known message and its encrypted form to obtain sufficient information about the encryption process. This information can then be used to decrypt or analyze other messages produced by the same method.
- Ciphertext-only attack – where the original plaintext is not accessible to the attacker, only the ciphertexts. Successfully performing this attack is generally difficult.
- Chosen-plaintext attack – the attacker has access to the ciphertext and the corresponding plaintext for several messages, and can choose plaintexts that are encrypted [3].
- Chosen-ciphertext attack – the attacker has access to ciphertexts and their corresponding plaintexts, and can also choose ciphertexts to be decrypted [3].

DOI: 10.25045/forensic.gov.2026.14

B. *Brute-force attack*

A brute-force attack is a systematic process of attempting every possible combination of passwords or cryptographic keys to gain unauthorized access to a system or data [4]. The size of the key has a direct impact on how effective a brute-force attack is. For small key sizes, brute-force attacks can be carried out very quickly. In fact, modern hardware can perform huge numbers of attempts per second. This makes such attacks very effective. However, it is necessary to mention that as key lengths increase, the number of combinations grows exponentially. This makes the attack impractical. For example, key size of 128 bits or higher are considered secure. It would take an excessive amount of time and computing power to brute-force systems with such key sizes. However, a brute-force attack can be effective if a weak password/key is used or repeated attempts are not restricted. To mitigate attack, it's necessary to take protective actions such as using long passwords/keys, adding delays between logins, and implementing CAPTCHA.

C. *Side-channel attack*

A side-channel attack is a type of security attack that tries to extract secret information by analyzing side information such as electromagnetic waves, acoustic signals, heat emission, power consumption, and execution time that are unintentionally emitted from a system [5]. These are further described below:

- **Electromagnetic waves** – when an electronic component is operating, electromagnetic radiation is released. By capturing and analyzing these emissions, attackers can gather important information.
- **Acoustic signals** – during the operation of the device, some electronic components produce sound waves. These sound waves can reveal sensitive information.
- **Heat emission** – each device produces some level of heat during operation. Moreover, the temperature of a system varies depending on the workload. It is possible to monitor temperature changes over time to gather some information about the system.
- **Power consumption** – depending on the functions it performs, a device's power consumption varies. Careful measurement of power consumption can reveal information about sensitive data.
- **Execution time** – each cryptographic operation takes a certain amount of time to execute. Attackers can measure these timing differences to gather valuable information about the system.

D. *MITM attack*

A MITM attack occurs when an attacker inserts themselves between communicating devices and intercepts the traffic exchanged between them [6]. The attacker can monitor, modify, and even delete the transmitted information. This type of attack can compromise the confidentiality and integrity of sensitive data. Sensitive data may include login credentials, banking transactions, private communications, and location data. Fig. 1 demonstrates the MITM attack process.

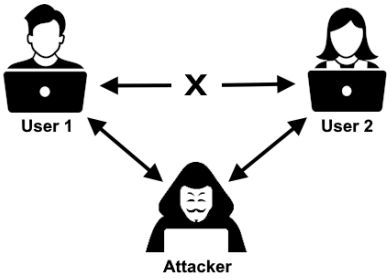

Figure 1. MITM attack process

MITM attacks can be very risky because they can happen even with encryption if the communication process isn't properly authenticated. One common example is public key exchange process in cryptographic systems. During the key exchange process, the attacker has the ability to intercept and provide their own public keys. As a result, the messages sent between the legitimate parties can be decrypted and read by the attacker [7].

III. Digital Forensic Analysis of Cryptographic Systems

Digital forensic analysis of cryptographic systems is the process of identifying, preserving, acquiring, analyzing, and reporting digital evidence from attacks that compromise cryptographic algorithms, protocols, or their implementations.

A. *Digital forensics analysis process of cryptographic systems*

The digital forensics analysis process for cryptographic systems is a specialized branch of digital forensics that consists of various steps. These steps are given below:

- **Identification:** The first step in digital forensic analysis is identification. This step includes encrypted files, cryptographic keys, digital certificates, and log files that may indicate how the system was compromised.
- **Preservation:** Preservation means protecting digital evidence from modification, damage, and erasure. This is achieved by using various methods such as write-blocking, securing storage, etc.
- **Acquisition:** Acquisition is the process of collecting the identified and preserved evidence. This step may include copying stored data, reading volatile memory, exporting log files, etc.
- **Analysis:** In this step, various tools are used to examine the acquired evidence. This helps to reconstruct events and determine how the cryptographic systems were attacked. Forensic investigators may recover cryptographic keys, examine digital certificates, and analyze log files for this task.
- **Reporting:** Reporting summarizes the findings of the forensic analysis. The report should describe what evidence was examined, how it was analyzed, and what was found.

B. *Evidence sources in cryptographic systems for digital forensic analysis*

Software, hardware, memory, and network activity can all provide evidence in investigations involving attacks on cryptographic systems. One of the highly valuable evidence sources is volatile memory (RAM). It could contain cryptographic keys, passwords, and plaintext data while a system is running [8]. By analyzing memory with special tools, investigators can sometimes recover the keys. Another highly valuable evidence source is persistence storages such as HDD, SSD, etc. They may contain digital certificate files, configuration files, and stored key files. System and application logs are also valuable evidence sources. They may include operating system logs, encryption software logs, and various service logs. These evidence sources may contain event records such as certificate issuance, key generation, and authentication attempts. Another important source is network traffic captures [9]. They include TLS handshakes, digital certificates, and various network metadata. In addition, there are various secure hardware devices such as Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), smart cards, etc. These devices could contain audit logs, stored key metadata, and other important data that can be helpful during an investigation. Cloud storage may also include important evidence such as encryption keys, access logs, and backups.

C. *Main tools for digital forensic analysis*

There are various tools for digital forensic analysis of cryptographic systems. These tools help investigators identify, preserve, collect, analyze, and report evidence related to attacks on cryptographic systems. Some of the main tools used for digital analysis are given below:

- Autopsy [10]: It's an open source digital forensics tool. This tool can recover deleted files, do timeline analysis, perform keyword searching, etc. A tool can be very useful to locate digital certificate files, private key files (.pfx, .pem, and other formats), and log files.
- EnCase Forensic [11]: This is a popular commercial digital forensic tool widely used by law enforcement. It helps investigators to collect and analyze data from hard drives, mobile phones, and cloud sources. EnCase Forensic can obtain a bit-by-bit copy of digital media while keeping all of the data on the storage device unchanged [12]. In investigations involving intrusions into cryptographic systems, this tool can be used to locate private key files, system logs, digital certificates, etc.
- FTK (Forensic Toolkit) [13]: This is one of the leading commercial digital forensics tools. It can be used to obtain, process, and analyze evidence from computers, mobile phones, and other digital sources. One of the main advantages of this tool is that it finds information more quickly than other available tools [14]. FTK can be used to locate private key files, digital certificates, etc.
- Volatility [15]: This is an open-source memory forensics tool. It helps investigators to extract running processes, network connections, and other important information that may not be present on persistence storages. In cryptographic forensic investigations, this tool can be used to recover encryption keys, passwords, and other vital data that exist temporarily in memory.
- Belkasoft X Forensic [16]: It is a digital forensic tool that can be used to collect and analyze evidence from computers, mobile phones, cloud services, and drones. The tool supports artifact extraction, RAM analysis, and timeline analysis. In investigations involving intrusions into cryptographic systems, Belkasoft X can be used to identify private keys, digital certificates, passwords, and browser artifacts.
- Magnet AXIOM [17]: It is a digital forensic tool designed to collect and analyze data from computers, mobile devices, cloud services, and removable media. The tool can extract artifacts such as deleted files, browser history, messages, emails, and system logs.
- Wireshark [18]: This is popular open-source packet analyzer software. Wireshark captures data packets as they move through a network in real time. It allows investigators to analyze secure communication protocols such as TLS/SSL, SSH, IPsec, and many others. It can help to identify suspicious traffic, handshakes, and certificate exchanges. Wireshark may still give useful metadata even when encrypted payloads cannot be directly read.
- Tcpdump [19]: This is a command-line packet capture tool used to analyze network traffic in real time. In cryptographic forensic investigations, tcpdump is used to collect raw traffic data that may contain evidence of attacks.
- Plaso [20]: It is an open-source digital forensics tool used to automatically build a forensic timeline. The tool can collect timestamps from sources such as file systems, event logs, and application logs. In investigations related to cryptographic intrusions, it can reconstruct attacker activity by correlating events such as key access, system logins, etc., in meaningful order.
- OpenSSL [21]: It is usually used to create keys, check certificates, and verify digital signatures. However, this tool may also be used by investigators to determine whether certificates were forged, expired, or misconfigured.
- Write-blocker [22]: This tool prevents writing any data to the storage device during the investigation, ensuring that the original evidence remains unchanged. It ensures private keys, digital certificates, and other important information will be collected without altering the original evidence.

IV. SECURİTY MEASURES FOR CRYPTOGRAPHİC SYSTEMS

Security measures for cryptographic systems help to prevent unauthorized access to sensitive data. They also reduce the impact of attacks on encryption mechanisms. Using strong

encryption algorithms is one of the most important security measures. Modern standards like the Advanced Encryption Standard (AES) are commonly used for encryption because they are secure. The security of cryptographic algorithms depends not only on their mathematical strength but also on selecting proper key lengths. Moreover, it is necessary to avoid using outdated algorithms. Attackers may be able to take advantage of known vulnerabilities in these algorithms with little effort. For example, algorithms like SHA-1, MD5, and DES are no longer considered secure. Therefore, outdated algorithms should be replaced with modern ones such as AES and SHA-256.

Secure key management is another important factor for the security of cryptographic systems. If encryption keys are exposed, even the most powerful encryption algorithm loses its effectiveness. It is recommended to use cryptographically secure random number generators when creating keys. Moreover, keys should be stored in secure environments such as HSMs. Only authorized users should be able to access keys. Also, all activities related to keys should be logged for auditing and forensic investigation. Moreover, backup copies of keys must be protected with the same level of security as the original keys. Organizations should also establish clear procedures for destroying keys when they are no longer needed.

It is also important to consider cyberattacks on cryptographic systems and take security measures. To mitigate brute-force attacks, systems should use large enough keys. It is also necessary to use strong key derivation functions such as Argon2 or scrypt. These mechanisms make each password guess more computationally expensive, making brute-force attacks much harder. Procedures like rate limiting and multi-factor authentication reduce the risk of successful brute-force attacks. Protection against MITM attacks can be achieved by using methods such as HTTPS Strict Transport Security (HSTS) and dynamic ARP inspection [23]. Other methods include mutual authentication, digital certificates, and the use of protocols such as TLS. Defense against side-channel attacks includes both hardware and software solutions. Main defense and mitigation strategies are constant-time execution, noise generation, masking, and blinding [24]. These techniques aim to reduce correlation between secret data and side-channel information (timing, power consumption, electromagnetic emissions, etc). In practice, effective protection often requires combining multiple security measures. Together, these security measures ensure that cryptographic mechanisms remain reliable.

CONCLUSION

This study examined the intrusion targeting cryptographic systems and the role of digital forensics in investigating them. The analysis showed that cryptographic systems remain vulnerable to various attacks. Understanding these attacks is important for identifying vulnerabilities and improving overall system security.

The paper also highlighted the importance of digital forensic analysis. It included a step-by-step digital forensics analysis process of cryptographic systems, evidence sources, and main tools used for digital forensic analysis. Finally, the study covered a number of ways to improve security of cryptographic systems.

REFERENCES

[1] R. Əliquliyev, Y. İmamverdiyev, "Kriptoqrafiyanın əsasları" Bakı, Azərbaycan: İnformasiya texnologiyaları, 2006.

[2] J. F. Dooley, "History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms," Cham, Switzerland: Springer Nature, 2024. doi:10.1007/978-3-031-67485-3

[3] B. Schneier, "Applied cryptography: Protocols, algorithms, and source code in C 2nd ed.," Nashville, TN: John Wiley & Sons, 1995.

[4] A. Eipper and D. Pöhn, "How to design a blue team scenario for beginners on the example of brute-force attacks on authentications," in Proceedings of the 9th International Conference on Information Systems Security and Privacy, 2023, pp. 477–484.

[5] T. Hirata and Y. Kaji, "Information leakage through passive timing attacks on RSA decryption system," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E106.A, no. 3, pp. 406–413, 2023. doi:10.1587/transfun.2022TAP0006

[6] E. D. Knapp and R. Samani, "Hacking the smart grid," in Applied Cyber Security and the Smart Grid, Elsevier, 2013, pp. 57–86. doi:10.1016/B978-1-59749-998-9.00003-7

[7] P. Radanliev, "Cyber-attacks on Public Key Cryptography," Preprints, 2023. doi:10.20944/preprints202309.1769.v1

[8] C. Maartmann-Moe, S. E. Thorkildsen, and A. Årnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys," Digital Investigation, vol. 6, pp. S132–S140, 2009.

[9] R. Mahajan and K. Pandit, "Cryptography and computational approaches in ensuring data integrity for digital forensic evidence," in 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2024.

[10] "Autopsy", https://www.autopsy.com/

[11] "EnCase", https://www.opentext.com/products/forensic

[12] S. Bunting, "EnCase computer forensics -- the official EnCE: EnCase certified examiner study guide 3rd ed.," Indianapolis, IN: Sybex, 2012.

[13] "Forensic Toolkit", https://www.exterro.com/digital-forensics-software/ftk-forensic-toolkit

[14] H. Himanshu, S. Bhatt, and L. Negi, "Digital Forensics techniques and trends: A review," The International Arab Journal of Information Technology, vol. 20, no. 4, 2023. doi:10.34028/iajit/20/4/11

[15] "Volatility", https://volatilityfoundation.org/the-volatility-framework/

[16] "Belkasoft X Forensic", https://belkasoft.com/x

[17] "Magnet AXIOM", https://www.magnetforensics.com

[18] "Wireshark", https://www.wireshark.org

[19] "Tcpdump", https://www.tcpdump.org

[20] "Plaso", https://github.com/log2timeline/plaso

[21] "Openssl", https://www.openssl.org

[22] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response (NIST SP 800-86)," National Institute of Standards and Technology, Gaithersburg, MD, 2006.

[23] D. S. Zhraw, M. A. Hussain, Z. A. Abduljabbar, V. O. Nyangaresi, and A. J. Y. Aldarwish, "Chronological review of MITM attacks: Challenges, solutions and recommendations," in Lecture Notes in Networks and Systems, Cham: Springer Nature Switzerland, 2025, pp. 202–220. doi:10.1007/978-3-032-03406-9_13

[24] M. D. M. Hassan, S. Roy, and R. Rahaeimehr, "Memory under siege: A comprehensive survey of side-Channel attacks on memory," Computers & Security, vol. 163, no. 104810, p. 104810, 2026.