TECH SCIENCE

ISSN 3030-3702

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

№ 3 (3) 2025

TECHSCIENCE.UZ

№ 3 (3)-2025

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

TOSHKENT-2025

OAK Ro‘yxati
Mazkur jurnal O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2025-yil 8-maydagi 370-son qarori bilan texnika fanlari bo‘yicha ilmiy darajalar yuzasidan dissertatsiyalar asosiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro‘yxatiga kiritilgan.

Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI
elektron jurnali 15.09.2023-yilda 130343-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com

TEXNIKA FANLARINING
DOLZARB MASALALARI
3-jild, 3-son (iyun, 2025). -116 bet.

M U N D A R I J A

Texnika fanlarining dolzarb masalalari
Topical Issues of Technical Sciences
2025-yil | 3-jild | 3-son
ISSN (onlayn): 3030-3702

ASSESSMENT OF CRYPTOGRAPHIC KEY GENERATION SYSTEMS USING DREAD AND STRIDE THREAT METHODOLOGIES

Nurullaev Mirkhon Muhammadovich
Doctoral student, Bukhara State Technical University
E-mail: nurullayevmirxon@gmail.com
Tel: +99897 303 34 49
ORCID: 0000-0001-7510-7628

Annotation. This article presents a comprehensive assessment of cryptographic key generation systems using the DREAD and STRIDE threat methodologies. The article concludes by highlighting the importance of these methodologies for developing secure cryptographic systems and outlines future directions for refining threat models using real-world data and predictive analytics.

Keywords: cryptographic key generation, DREAD methodology, STRIDE methodology, risk assessment, threat analysis, information security, mathematical modeling

DREAD VA STRIDE TAHDID METODOLOGIYALARIDAN FOYDALANIB KRIPTOGRAFIK KALITLARNI GENERATSIYALASH TIZIMLARINI BAHOLASH

Nurullayev Mirxon Muhammadovich
Buxoro davlat texnika universiteti tayanch doktoranti

Annotatsiya. Ushbu maqola DREAD va STRIDE tahdid metodologiyalaridan foydalangan holda kriptografik kalit yaratish tizimlarining keng qamrovli baholashga bag‘ishlangan. Maqola ushbu metodologiyalarning xavfsiz kriptografik tizimlarni ishlab chiqish uchun ahamiyatini ta’kidlab, haqiqiy ma’lumotlar va bashorat tahlillari yordamida tahdid modellarini takomillashtirish uchun kelajakdagi yo‘nalishlarini belgilaydi.

Kalit so‘zlar: kriptografik kalit yaratish, DREAD metodologiyasi, STRIDE metodologiyasi, xavfni baholash, tahdid tahlili, axborot xavfsizligi, matematik modellashtirish

DOI: https://doi.org/10.47390/issn3030-3702v3i3y2025N03

Introduction

The issue of creating cryptographic keys is a key component of modern Information Security, which serves as the basis for ensuring the security of communication and protecting data. However, as noted by Shostack [1] and Stallings [2], these systems are increasingly vulnerable to complex cyber threats such as spoofing, tampering, denial of service type attacks. By modeling threats, however, it should be noted that these vulnerabilities are regularly identified and as a crucial tool for their elimination. Despite the development of cryptographic protocols, studies show that certain gaps remain in the elimination of the full spectrum of threats. These loopholes can lead to threats to the confidentiality, integrity and availability for cryptographic key generation systems. For example, Naik et al. [3]

demonstrating the limitations of traditional methods of risk assessment when applied to modern cryptographic systems, it is emphasized that improved threat modeling techniques are needed. This article focuses on the problem of protecting cryptographic key generation systems against various threats using the Stride [4] and DREAD [5] methodologies. The STRIDE methodology provides a structured framework for classifying threats [6], while the DREAD methodology allows quantitative assessment of threats [7]. Combining the above approaches, this research work develops the cryptographic security level [8-9] to offer a comprehensive solution to the identified problem.

Methods

1. STRIDE methodology

The STRIDE methodology developed by Microsoft is a widely used approach to regularly identify and classify security threats [10]. STRIDE is derived from the first letters of words representing a particular type of threat, meaning Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

Each threat category is systematically analyzed by determining the probability and severity of occurrence [11].

Assessment using STRIDE

The STRIDE methodology categorizes threats into 6 distinct types. Below (Table 1) is an example assessment for a cryptographic key generation system.

Table 1.

Assessment for a cryptographic key generation system

Threat Category	Description	Example Threat	Mitigation Strategy
Spoofing	Impersonating a legitimate user or system.	An attacker bypasses authentication to access the key generation module.	Implement strong authentication (e.g., MFA, biometric verification).
Tampering	Unauthorized modification of data or processes.	Malicious software alters the entropy source used for key generation.	Use hardware-based random number generators with integrity checks.
Repudiation	Denying having performed an action or transaction.	A user denies generating a specific key.	Use detailed logging and digital signatures for audit trails.
Information Disclosure	Unauthorized access to sensitive data.	An attacker intercepts the generated keys during transmission.	Encrypt keys during transmission using secure protocols (e.g., TLS).
Denial of Service	Disrupting or preventing legitimate system use.	Repeated API requests overwhelm the key generation service.	Implement rate limiting and DDoS protection.
Elevation of Privilege	Gaining unauthorized access to higher	A low-privilege user exploits a vulnerability to access the key generation	Apply the principle of least privilege (PoLP) and regularly update security

	privileges.	system as an administrator.	patches.

Each threat type in STRIDE is evaluated using probabilities and mitigation strategies. Let:

- $P(T_i)$: Probability of a specific threat T_i occurring.
- $S(T_i)$: Severity of threat T_i if exploited.
- $R(T_i)$: Risk score for threat T_i, computed as:

$$R(T_i) = P(T_i) \times S(T_i)$$

2. DREAD methodology

The DREAD methodology provides a quantitative framework for evaluating the risks associated with each identified threat. DREAD stands for Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability, which are scored individually to determine the overall risk.

To enhance precision, weighted scoring can be applied, where each criterion is assigned a weight based on its relative importance:

This allows for a nuanced analysis, prioritizing high-impact threats that require immediate mitigation [5].

For each threat T_i, DREAD assigns scores for **Damage (D)**, **Reproducibility (R)**, **Exploitability (E)**, **Affected Users (A)**, and **Discoverability (D)**. The overall risk score $R(T_i)$ is the average (Table 2) of these components:

$$R(T_i) = \frac{D(T_i) + R(T_i) + E(T_i) + A(T_i) + D(T_i)}{5}$$

Where:

- $D(T_i)$: Damage potential
- $R(T_i)$: Reproducibility
- $E(T_i)$: Exploitability
- $A(T_i)$: Affected users
- $D(T_i)$: Discoverability

Table 2.

DREAD risk calculation

Threat	**D**	**R**	**E**	**A**	**D**	**Risk** $R(T_i)$
Spoofing	8	6	7	9	5	7.0
Tampering	9	5	6	7	4	6.2
Information Disclosure	7	7	8	9	6	7.4
Denial of Service (DoS)	5	8	9	10	6	7.6
Elevation of Privilege	9	6	7	8	6	7.2

Assessment using DREAD

The DREAD model quantifies the risk of each threat by scoring it based on five factors. The scores typically range from 1 (low) to 10 (high). Below (Table 3) is an example assessment:

Table 3.

Assessment Using DREAD

Threat	Damage Potential (D)	Reproducibility (R)	Exploitability (E)	Affected Users (A)	Discoverability (D)	Total Score	Risk Level
Spoofing user authentication	8	6	7	9	5	35	High
Tampering with entropy source	9	5	6	7	4	31	High
Information disclosure via interception	7	7	8	9	6	37	Critical
Denial of Service (DoS)	5	8	9	10	6	38	Critical
Elevation of privilege	9	6	7	8	6	36	Critical

Explanation of Scores:

1. **Damage Potential (D)**: The impact of the threat on the system if it is successfully executed.
2. **Reproducibility (R)**: The likelihood of the threat being replicated by attackers.
3. **Exploitability (E)**: The ease with which the threat can be exploited.
4. **Affected Users (A)**: The number of users impacted by the threat.
5. **Discoverability (D)**: How easily the threat can be discovered by attackers.

Risk Levels:

- **Critical (35-50)**: Requires immediate mitigation.
- **High (25-34)**: Should be addressed as soon as possible.
- **Medium (15-24)**: Monitor and address if resources permit.
- **Low (1-14)**: Acceptable risk, but consider long-term improvements.

Mathematical formalization of the threat model for random number generators.

The security of cryptographic systems fundamentally depends on the quality of their random number generators (RNGs) [12]. To rigorously analyze the security threats to RNG systems, we propose a comprehensive mathematical formalization of the threat model. This formalization allows for precise reasoning about security properties, vulnerabilities, and attack vectors in the context of random number generation.

Random number generation model

$$\mathrm{R}_n = f(s, \mathrm{R}_{n-1}, \mathrm{E}_n)$$

Where:

- R_n - is the n-th generated random number
- s - is the initial seed value
- R_{n-1} - is the previously generated random number
- E_n - is the n-th entropy input
- f - is the generation function

State transition function

The internal state transition of the RNG can be modeled as:

$$S_n = g(S_{n-1}, E_n)$$

Where:

- $\mathbf{S_n}$ is the state of the RNG after the n-th iteration
- **g** is the state transition function

Weighted risk formula

For a more detailed risk calculation, assign weights $\omega_D, \omega_R, \omega_E, \omega_A, \omega_D$ to each DREAD factor based on the system's criticality:

$$R(T_i) = \omega_D \cdot D(T_i) + \omega_R \cdot R(T_i) + \omega_E \cdot E(T_i) + \omega_A \cdot A(T_i) + \omega_D \cdot D(T_i)$$

For example, if weights are:

$$\omega_D = 0.3, \omega_R = 0.2, \omega_E = 0.2, \omega_A = 0.2, \omega_D = 0.1,$$

For **Spoofing**:

$$R(\text{Spoofing}) = 0.3 \cdot 8 + 0.2 \cdot 6 + 0.2 \cdot 7 + 0.2 \cdot 9 + 0.1 \cdot 5 = 7.1$$

Overall risk for the system

The overall system risk R_{System} is the sum of individual threat risks:

$$R_{System} = \sum_{i=1}^{n} R(T_i)$$

Using the STRIDE:

$$R_{System} = 2.4 + 3.6 + 1.4 + 5.0 + 4.8 + 2.7 = 19.9$$

For DREAD:

$$R_{System} = 7.0 + 6.2 + 7.4 + 7.6 + 7.2 = 35.4$$

3. Integrating STRIDE and DREAD

By integrating STRIDE and DREAD, a comprehensive risk assessment framework is developed. STRIDE categorizes threats and identifies vulnerabilities, while DREAD quantifies the associated risks, enabling prioritized mitigation. For instance, a STRIDE analysis may identify information disclosure as a critical threat, which is then evaluated using DREAD to determine its risk score and prioritize countermeasures such as enhanced encryption protocols [13].

Results

STRIDE risk assessment

The STRIDE methodology was applied to evaluate potential threats to the cryptographic key generation system [14]. For each identified threat, the probability of occurrence and severity were estimated. The resulting risk scores are summarized below (Table 4):

Table 4.

Resulting risk scores

Threat Category	Probability	Severity	Risk
Spoofing	0.3	8	2.4
Tampering	0.4	9	3.6
Repudiation	0.2	7	1.4
Information Disclosure	0.5	10	5.0
Denial of Service (DoS)	0.6	8	4.8
Elevation of Privilege	0.3	9	2.7

The STRIDE analysis revealed that **Information Disclosure** and **Denial of Service (DoS)** have the highest risk scores, highlighting their critical nature. Below (Fig.) is a bar chart illustrating the STRIDE risk score. It shows the risk scores for each threat category, helping you visually compare their relative severity [15].

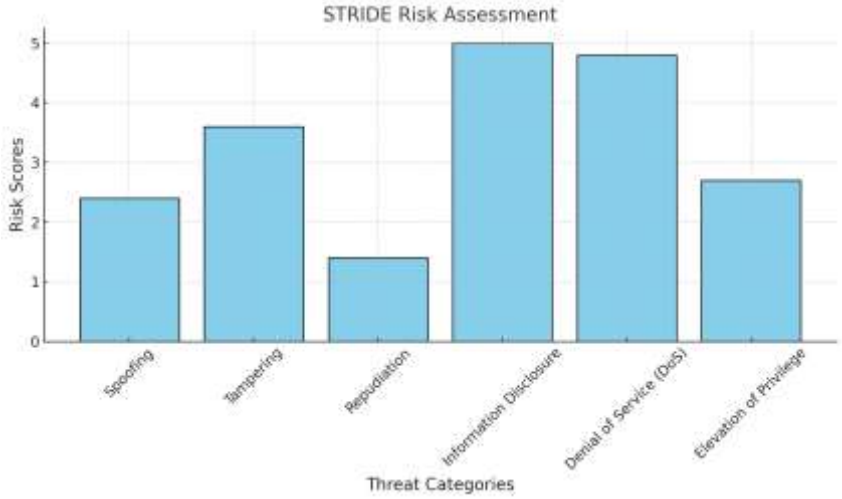

FIGURE. STRIDE Risk Assessment

DREAD risk assessment

The DREAD methodology further quantified the risks by assigning individual scores to each of the five criteria for each identified threat. The results are summarized as follows (Table 5):

Table 5.

Summarized results

Threat	D	R	E	A	D	Risk
Spoofing	8	6	7	9	5	7.0
Tampering	9	5	6	7	4	6.2
Information Disclosure	7	7	8	9	6	7.4
Denial of Service (DoS)	5	8	9	10	6	7.6
Elevation of Privilege	9	6	7	8	6	7.2

The **Denial of Service (DoS)** threat yielded the highest risk score (7.6), followed by **Information Disclosure** (7.4). These findings align with the STRIDE results, underscoring the need for targeted mitigation strategies.

Overall risk assessment

The combined results from STRIDE and DREAD provide a clear prioritization of threats. By integrating qualitative and quantitative analyses, this comprehensive approach ensures that critical risks are effectively addressed, thus enhancing the security of cryptographic key generation systems [16].

Discussion

The findings from the STRIDE and DREAD assessments provide a scientifically robust framework for identifying and mitigating security threats in cryptographic key generation systems. The integration of these methodologies enables a dual-layered analysis, where STRIDE helps to systematically categorize potential threats, and DREAD offers a quantitative assessment of their risks. This combined approach ensures that organizations can effectively prioritize mitigation strategies based on both the nature and severity of the threats.

The analysis revealed that **Information Disclosure** and **Denial of Service (DoS)** pose the highest risks to cryptographic key generation systems. These findings are consistent with prior research [11, 17], which highlights the critical impact of data leaks and system unavailability on overall security. Addressing these threats requires robust countermeasures, such as implementing advanced encryption protocols to protect sensitive data and deploying rate-limiting techniques to mitigate DoS attacks [18].

Another significant contribution of this study is the use of mathematical models to calculate risk scores, ensuring transparency and reproducibility in the assessment process. The weighted scoring system in the DREAD framework further enhances the precision of risk evaluations, allowing for the tailored prioritization of high-impact threats.

The results also emphasize the need for ongoing refinement of threat modeling methodologies. Incorporating real-world data and leveraging machine learning algorithms could improve the predictive accuracy of these models, enabling proactive threat detection and mitigation. Moreover, future research could explore the integration of additional methodologies, such as PASTA or LINDDUN, to provide a more comprehensive security analysis [10].

In conclusion, this study demonstrates the efficacy of combining STRIDE and DREAD methodologies for securing cryptographic key generation systems. By systematically identifying and quantifying risks, organizations can implement targeted and effective countermeasures to enhance the security of their systems [19, 20]. These findings contribute to the broader field of information security and underscore the importance of continuous advancements in threat modeling and risk assessment techniques.

Conclusion

This study demonstrated the effectiveness of integrating the STRIDE and DREAD methodologies to systematically assess and mitigate threats to cryptographic key generation systems. STRIDE offered a structured framework for categorizing potential threats, enabling a detailed analysis of vulnerabilities, while DREAD provided a quantitative evaluation of the associated risks. This dual-methodology approach facilitates the prioritization of high-impact threats, ensuring that the most critical risks, such as Information Disclosure and Denial of Service (DoS), are addressed promptly.

The findings highlight the importance of implementing advanced encryption mechanisms, robust authentication protocols, and resource management strategies to mitigate these critical threats. Additionally, the use of mathematical modeling in DREAD ensures transparency, reproducibility, and precision in risk assessment, laying a solid foundation for evidence-based decision-making in security planning.

Future research should aim to enhance the predictive accuracy of these models by incorporating real-world threat data and leveraging emerging technologies such as machine learning. Furthermore, integrating additional threat modeling methodologies, such as PASTA and LINDDUN, could provide a more comprehensive security analysis, further strengthening the resilience of cryptographic key generation systems.

In conclusion, this research contributes to advancing the field of information security by providing a scientifically rigorous and practical framework for threat assessment. By continuously refining and expanding these methodologies, organizations can build more secure systems, ensuring the integrity, confidentiality, and availability of cryptographic processes in an increasingly hostile cyber environment.

Adabiyotlar/Литература/References:

1. Shostack, A. Threat Modeling: Designing for Security. Wiley, 2014.
2. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
3. Naik, N., & Jenkins, P. "Towards Analysis of Threat Modeling of Software Systems: A Comparative Study." Springer, 2024.
4. Microsoft Corporation. "The STRIDE Threat Model." Retrieved from [Microsoft Documentation], 2003.
5. OWASP. "DREAD Risk Assessment Model." Retrieved from [OWASP Documentation], 2023.
6. Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe) (pp. 1-6). IEEE, 2018. https://doi.org/10.1109/ISGTEurope.2018.8571516
7. Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. Threat modelling methodologies: A survey. IEEE Access, 9, 4422-4445, 2021. https://doi.org/10.1109/ACCESS.2020.3047368
8. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2020.
9. Mitropoulos, F., & Spinellis, D. "Threat Modeling Methodologies for Cryptographic Systems." ACM Computing Surveys, 54(4), 1-32. 2022.
10. Naik, N., Jenkins, P., & Grace, P. "A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN." TechRxiv, 2024.
11. Omotosho, A., et al. "STRIDE-Based Cybersecurity Threat Modeling, Risk Assessment and Mitigation for IoT-Enabled Precision Agriculture." arXiv preprint arXiv:2201.09493, 2022.
12. Pauget, F., Lacombe, A., & Grigoleit, F. Strengthening cryptographic key derivation using proof-of-work. Journal of Information Security and Applications, 54, 102562, 2020. https://doi.org/10.1016/j.jisa.2020.102562
13. Kuznetsov, O., Zakharov, D., & Frontoni, E. "Deep Learning-Based Biometric Cryptographic Key Generation with Post-Quantum Security." Multimedia Tools and Applications, 2023.
14. Scandariato, R., Wuyts, K., & Joosen, W. A descriptive study of Microsoft's threat modeling technique. Requirements Engineering, 20(2), 163-180, 2015. https://doi.org/10.1007/s00766-013-0195-2
15. Labunets, K., Paci, F., Massacci, F., & Ruprai, R. An experiment on comparing textual vs. visual industrial methods for security risk assessment. In 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS) (pp. 105-112). IEEE, 2017. https://doi.org/10.1109/QRS.2017.20
16. Amini, P., Araghizadeh, M. A., & Azmi, R. A survey on adversarial attacks and defenses in text classification. International Journal of Machine Learning and Cybernetics, 10(10), 2059-2069, 2019. https://doi.org/10.1007/s13042-019-00931-8
17. Nurullaev M.M. "Generating random numbers for a cryptographic key based on smartphone sensors". International Scientific and Practical Conference on "Modern Problems of Applied Mathematics and Information Technology (MPAMIT2022)" AIP Conf. Proc. 3004, 060014-1–060014-5; 2024. https://doi.org/10.1063/5.0199570
18. Staat, P., et al. "Intelligent Reflecting Surface-Assisted Wireless Key Generation for Low-Entropy Environments." arXiv preprint arXiv:2010.06613, 2020.
19. Nurullaev M. M. "Functions and their mechanisms for generating cryptographic keys and random numbers," AIP Conference Proceedings 2969, 2024. (AIP Publishing, Melville, NY). https://doi.org/10.1063/5.0181797.

20. Tete, S. B. “Threat Modelling and Risk Analysis for Large Language Model (LLM)-Powered Applications.” arXiv preprint arXiv:2406.11007. 2024.

ISSN: 3030-3702 (Online)
САЙТ: https://techscience.uz

TECHSCIENCE.UZ

TEXNIKA FANLARINING DOLZARB MASALALARI

№ 3 (3)-2025

TOPICAL ISSUES OF TECHNICAL SCIENCES

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI elektron jurnali 15.09.2023-yilda 130343-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.
Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com