ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Technical Research Center

Cybersecurity Risk by Design (CRD): Integrating DRM and DTM for Enhanced Threat Modeling

Research Paper: ISAU-RP-907-2025-CRD

ISAU-TG57-2025
6-16-2025

An ISAUnited.org Published Whitepaper

Institute of Security Architecture United (ISAUnited.org)

Author or Task Group Number:

ISAU-TG57-2025

Publishing Reviewer(s):

ISAUnited Master Fellow Committee

Affiliation: ISAUnited.org

Date:

June 16, 2025

Document Registration Number:

ISAU-RP-907-2025-CRD

Assigned by the Institute Document Management Register

Cybersecurity Risk by Design (CRD): Integrating DRM and DTM for Enhanced Threat Modeling

ISAUnited Research Paper

Abstract

The Cybersecurity Risk by Design (CRD) model represents a transformative enhancement to threat modeling practices within cybersecurity engineering. Integrating structured methodologies from traditional engineering disciplines—specifically, the Design Risk Model (DRM) and the Design Threat Model (DTM) —CRD addresses fundamental shortcomings that have historically limited the effectiveness of threat modeling. Current cybersecurity breaches highlight persistent gaps, which are exacerbated by the rapidly evolving complexities of advancements such as artificial intelligence (AI) and cloud infrastructures. Drawing upon cross-disciplinary expertise from civil, aerospace, and systems engineering, the CRD model proactively identifies, analyzes, and mitigates threats systematically from the earliest stages of design. Aligned closely with the mandatory threat modeling guidelines advocated by the National Institute of Standards and Technology (NIST), this approach provides cybersecurity engineers with a structured, defensible framework to dramatically enhance the accuracy and efficacy of threat modeling processes. Empirical evidence underscores substantial benefits, including significantly reduced vulnerabilities, improved cost efficiency, and strengthened operational resilience. Further augmented by intelligent engineering, which continuously integrates real-time threat intelligence and advanced analytics, the CRD model equips organizations with predictive capabilities and adaptive resilience, critical for securely managing contemporary, complex technological environments.

Key words: Cybersecurity Risk by Design (CRD), Design Risk Model (DRM), Design Threat Model (DTM), Intelligent Engineering, Threat Modeling (TM), Cybersecurity Engineering, Proactive Risk Mitigation, Artificial Intelligence (AI), Cloud Security, Operational Resilience, Cross-Disciplinary Engineering.

Introduction

The integration of cybersecurity risk assessment into the design phase, specifically through the use of structured Design Risk Models (DRMs) and Design Threat Models (DTMs), addresses this gap. The Cybersecurity Risk by Design (CRD) model provides a comprehensive approach by combining these two essential frameworks.

Problem Statement

Organizations today face increasingly sophisticated cybersecurity threats, exemplified by recent high-profile incidents such as the SolarWinds supply chain attack (2020) and the Log4j vulnerability (2021). These incidents illustrate how architectural vulnerabilities and inadequate threat modeling can result in significant breaches and operational disruptions. Despite substantial investments in cybersecurity tools and controls, organizations continue to experience violations primarily due to insufficient initial design assessments and gaps in threat modeling practices. Historically, cybersecurity engineering has lacked structured and defensible methodologies, akin to those rigorously applied in traditional engineering disciplines, resulting in systems that are inherently vulnerable by design. The National Institute of Standards and Technology (NIST) now emphasizes the mandatory implementation of Threat Modeling (TM) as a core practice within comprehensive cybersecurity programs, advocating early and systematic identification and mitigation of threats throughout the system lifecycle [1].

Complexity of Modern Architectures

Modern architectural designs increasingly incorporate advanced technologies, notably artificial intelligence (AI), cloud computing, microservices, containerization, and serverless infrastructures. These innovations, while delivering enhanced efficiency and scalability, substantially increase the complexity and potential attack surface of organizational systems.

Rapid technological advancements, particularly the accelerated integration of AI-driven capabilities across various sectors, introduce new vulnerabilities and sophisticated threat vectors. AI's capabilities, such as machine learning algorithms and automation, are increasingly utilized by malicious actors to conduct targeted attacks, automate threat discovery, and evade detection mechanisms. According to IBM's Cost of a Data Breach Report (2022), organizations leveraging AI and cloud-based technologies are encountering increasingly costly breaches due to the sophistication and complexity of contemporary attack methods [3].

Furthermore, cloud-native technologies and microservices architecture create highly distributed environments that complicate traditional security management practices, demanding more dynamic and adaptable security approaches.

This escalating complexity underscores the urgent need for robust cybersecurity frameworks that can proactively address these emerging threats. Traditional cybersecurity measures, typically reactive and less structured, are insufficient for securing modern, sophisticated infrastructures. The integration of structured risk management methodologies, such as DRM, alongside proactive threat modeling, becomes crucial for effectively securing these rapidly evolving technological landscapes. ISAUnited's structured, disciplined approach to cybersecurity risk management, as evidenced by the adoption of DRM and proactive threat modeling, provides organizations with the necessary tools to mitigate risks effectively, despite the growing complexity and rapid pace of technological advancement.

Collaboration with Traditional Engineering Disciplines

ISAUnited.org recognized the critical need for enhanced rigor in cybersecurity engineering practices and proactively engaged experienced professionals from traditional engineering disciplines, notably civil, aerospace, and systems engineering, to assess and address existing gaps in cybersecurity methods. This intentional cross-disciplinary approach highlighted a significant oversight within cybersecurity: many cybersecurity engineers do not consistently or systematically implement structured threat modeling processes during the architectural design and development phases, resulting in preventable vulnerabilities and operational risks.

Traditional engineering fields, exemplified by aerospace, civil, and systems engineering, have effectively utilized structured methodologies, such as Design Risk Management (DRM), for decades. DRM facilitates comprehensive risk identification, assessment, and mitigation at the earliest stages of project design, significantly improving safety, reliability, and performance outcomes. For example, the aerospace industry's adoption of DRM methodologies has been extensively documented and formalized in resources such as NASA's Risk Management Handbook [2]. This handbook explicitly outlines a rigorous approach for systematically anticipating and addressing potential risks before they materialize, resulting in improved outcomes and significantly reduced risk exposure.

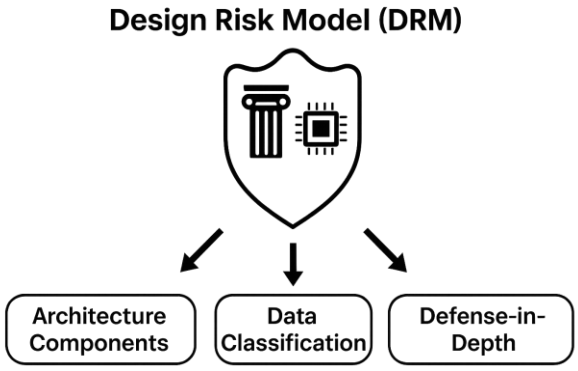
By integrating these proven DRM methodologies from traditional engineering disciplines into cybersecurity practices, ISAUnited.org aims to elevate the maturity, effectiveness, and defensibility of cybersecurity engineering. This cross-disciplinary integration fosters

a culture of proactive risk mitigation, ensuring that cybersecurity practices evolve to address increasingly sophisticated and complex threats faced by modern organizations.

Importance of DRM and DTM

Design Risk Model (DRM)

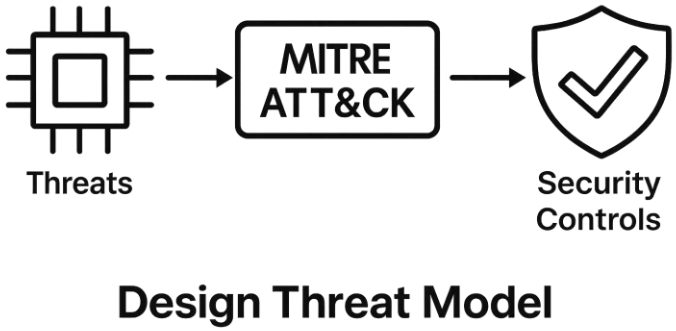
The Design Risk Model evaluates inherent risks systematically based on critical architecture components, data classification sensitivity, and defense-in-depth positioning within the architecture. By proactively identifying potential points of vulnerability, DRM enables architects and engineers to mitigate risks during the design phase, long before adversaries can exploit them. The methodical approach of DRM aligns cybersecurity engineering more closely with the structured, proactive risk assessments that have long been standard practice in traditional engineering fields, such as civil, aerospace, and systems engineering. This alignment ensures rigorous identification and management of structural vulnerabilities, thus significantly enhancing the security and resilience of designed systems.



Design Threat Model (DTM)

The Design Threat Model complements DRM by explicitly identifying potential threats through the utilization of standardized, industry-recognized frameworks such as MITRE ATT&CK. DTM systematically pinpoints specific threats, outlines precise threat actor behaviors, and provides clear, actionable threat mitigation strategies. The practical value of DTM lies not only in threat identification but also in ensuring that identified security controls are effectively implemented, continuously monitored, and their effectiveness objectively assessed. Incorporating DTM into cybersecurity practices guarantees comprehensive threat visibility, enabling organizations to dynamically adjust

their defenses in response to evolving threat landscapes and maintain a strong, adaptable security posture.



Intelligent Engineering

Intelligent engineering represents a proactive evolution in cybersecurity, integrating real-time threat intelligence and advanced analytics directly into the cybersecurity engineering lifecycle. By continuously assimilating and analyzing emerging threats, vulnerabilities, and malicious patterns, intelligent engineering allows organizations to dynamically adjust their security posture, preemptively mitigating risks before they can be exploited.

Continuous integration of threat intelligence involves leveraging data feeds from reputable sources, including MITRE ATT&CK, Cybersecurity & Infrastructure Security Agency (CISA), and vendor-specific intelligence streams. This intelligence, coupled with advanced analytical methods such as machine learning (ML) and artificial intelligence (AI), enables cybersecurity systems to rapidly detect anomalies, predict potential attack vectors, and facilitate swift remediation actions. According to Gartner (2023), organizations adopting continuous threat intelligence and analytics experience significantly reduced response times to security incidents and enhanced resilience against evolving threats [4].

This intelligent approach also supports automated threat modeling, where identified intelligence automatically informs and updates threat models, enabling real-time risk management and enhanced decision-making processes. As cyber threats become increasingly sophisticated and pervasive, incorporating intelligent engineering practices into cybersecurity engineering is crucial for maintaining robust defenses and adaptable security architectures.

Evidence and Benefits

The adoption of structured cybersecurity risk methodologies, specifically through integrated Design Risk Models (DRM) and Design Threat Models (DTM), has demonstrated substantial benefits in terms of vulnerability reduction, operational efficiency, and cost savings. Empirical studies and industry research consistently highlight the tangible benefits that organizations realize when they systematically apply these structured cybersecurity practices.

According to the Ponemon Institute's Cost of a Data Breach Report (2022), organizations implementing robust threat modeling and structured risk management frameworks experienced a significant decrease in both the frequency and impact of cybersecurity incidents. The report specifically noted that systematic threat modeling can lead to an average cost reduction of nearly 40% per incident, primarily due to earlier detection and more effective mitigation strategies [3].

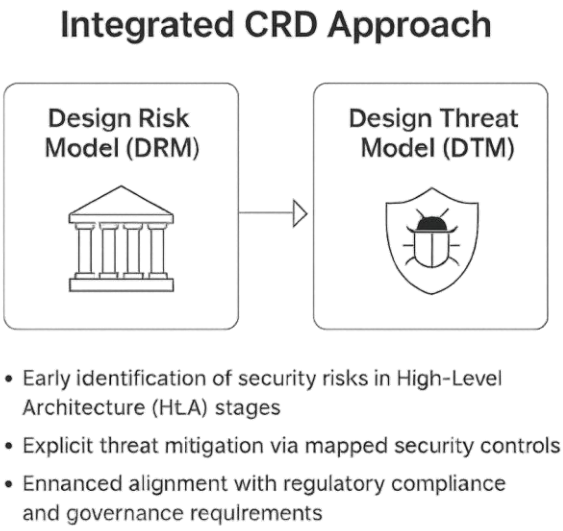
Furthermore, structured risk management frameworks such as those employed in aerospace and civil engineering, documented by NASA (2020), have proven highly effective in systematically identifying, evaluating, and mitigating risks early in the design phase, thereby drastically reducing the potential for costly failures or incidents [2]. These engineering disciplines consistently report improved reliability, reduced vulnerabilities, and substantial long-term cost savings.

Integrating DRM and DTM practices within cybersecurity engineering not only addresses immediate security concerns but also significantly enhances overall organizational resilience and compliance posture. Organizations that proactively adopt these methodologies demonstrate measurable improvements in security performance metrics, reduced financial and reputational risks, and improved stakeholder confidence.

Integrated CRD Approach

Combining DRM and DTM into the CRD model provides a holistic risk assessment:

- Early identification of security risks in High-Level Architecture (HLA) stages.
- Explicit threat mitigation via mapped security controls.
- Enhanced alignment with regulatory compliance and governance requirements.



Mandatory Requirement of Threat Model

Threat modeling (TM) has evolved from being an optional practice to a mandatory component within comprehensive cybersecurity programs, as emphasized by the National Institute of Standards and Technology (NIST). This mandatory status is driven by the increasing complexity of cybersecurity threats and the need for early and proactive intervention to effectively reduce vulnerabilities. According to NIST's Special Publication 800-160, systematic threat modeling must be integrated early into the system lifecycle to anticipate, identify, and mitigate potential security threats before they materialize, significantly enhancing an organization's resilience and security posture [1]. Historically, cybersecurity approaches have often focused on reactive measures implemented after an incident, leading to increased operational disruptions, financial losses, and reputational damage. Recent high-profile incidents, such as the SolarWinds and Log4j breaches, have underscored the consequences of insufficient threat modeling and the resulting vulnerabilities that arise from inadequate initial security assessments.

The shift towards mandatory TM underscores the necessity for structured, defensible practices that systematically address security risks at the earliest stages of the design process. Effective threat modeling incorporates scenario-based analyses, leveraging standardized frameworks such as MITRE ATT&CK, to comprehensively understand and prioritize threats. By mandating threat modeling, organizations are compelled to adopt rigorous cybersecurity engineering standards, enhancing their capacity to foresee and prevent security incidents.

This regulatory imperative is not merely compliance-driven but is rooted deeply in the practical benefits observed in structured threat modeling implementations. These

benefits include significantly reduced incident rates, improved system reliability, lower costs associated with incident response and remediation, and an overall stronger, more adaptive cybersecurity posture.

Thus, the mandatory requirement of threat modeling advocated by NIST aligns cybersecurity engineering with established practices from traditional engineering disciplines, ensuring proactive and systematic risk mitigation that is essential in modern digital environments.

Future Recommendations

- Regular CRD model updates are aligned with evolving cybersecurity threats and standards.
- Continuous integration with CI/CD pipelines for automated security assessments.
- Further engagement with cross-disciplinary engineering practices for continuous improvement.

Conclusion

The Cybersecurity Risk by Design (CRD) model, integrating Design Risk Models (DRM) and Design Threat Models (DTM), represents a modern and mature approach to cybersecurity engineering. It ensures security by design, enabling organizations to secure their architecture and infrastructure proactively. By systematically addressing cybersecurity risks early in the design phase, CRD significantly reduces vulnerabilities, aligns with regulatory mandates, and enhances overall organizational resilience.

Adopting the CRD model positions organizations at the forefront of cybersecurity practices, ensuring they remain resilient against increasingly sophisticated and evolving threats. This proactive approach not only mitigates risks effectively but also provides tangible benefits such as reduced operational disruptions, cost savings, and enhanced stakeholder trust. As cybersecurity threats continue to escalate, integrating structured, intelligence-driven frameworks like CRD will become essential for any organization committed to safeguarding its digital infrastructure and maintaining operational integrity in today's complex technological landscape.

References

1. National Institute of Standards and Technology. (2023). Special Publication 800-160, Volume 1: Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
2. NASA. (2020). Risk Management Handbook (NASA/SP-2020-5007). This handbook outlines systematic risk identification, evaluation, and mitigation strategies used in traditional engineering disciplines such as aerospace and systems engineering. Retrieved from https://ntrs.nasa.gov/citations/20205006278
3. Ponemon Institute. (2022). Cost of a Data Breach Report 2022. Retrieved from https://www.ibm.com/security/data-breach
4. Gartner. (2023). Top Strategic Technology Trends for 2023: Cybersecurity Mesh Architecture. Retrieved from https://www.gartner.com/en/documents/4029836

End of Document.

IO.