

BRIDGING MISUSE CASE MODELING AND MITRE ATT&CK: A UNIFIED FRAMEWORK FOR THREAT-INFORMED DESIGN

Jean-Marie Kabasele Tenday

Department of Computer Science, University ND Kasayi(UKA), Kananga, DR
Congo. DR Congo

ABSTRACT

Traditional threat modeling techniques often focus on theoretical or system-specific threats without grounding them in empirical adversarial behavior. Conversely, frameworks such as MITRE ATT&CK provide rich, intelligence-based taxonomies of real-world attacker tactics, techniques, and procedures (TTPs), but are rarely integrated into early software design phases. This paper proposes a methodology for linking misuse cases—UML-based representations of malicious system interactions—with MITRE ATT&CK techniques, enabling traceability between system-level threats and empirically observed attacks. The proposed framework enhances the relevance, completeness, and operational value of misuse case-based threat modeling. A structured mapping template and example implementation demonstrate how software architects can enrich their security design processes using ATT&CK-informed misuse cases.

KEYWORDS

Misuse case, MITRE ATT&CK, Threat Analysis, Threat Modeling, Cybersecurity, Secure Design.

1. INTRODUCTION

Software systems increasingly face complex and evolving cyber threats. Security by design has therefore become a cornerstone of modern engineering practices. Among available techniques, misuse case modeling provides an intuitive mechanism for representing how malicious actors could exploit system functionalities. However, traditional misuse case models are often disconnected from threat intelligence frameworks, limiting their realism and operational value. This paper proposes a systematic linkage between misuse cases and the MITRE ATT&CK framework to make threat modeling more actionable by grounding theoretical misuse scenarios in real-world adversarial data.

The paper is structured as follows: Section 2 discusses related work, including misuse case modeling and ATT&CK-driven threat modeling. Section 3 introduces the proposed methodology. Section 4 presents a practical case study and details the ATT&CK workflow, Section 5 explores future work and Section 6 concludes the paper.

2. RELATED WORK

2.1. Misuse Case Modeling

The misuse case concept, introduced by Sindre and Opdahl (2000, 2005), extends the traditional UML use case model to represent unwanted or malicious interactions with a system. While use cases describe legitimate user objectives, misuse cases capture how attackers could exploit system functionalities for harmful purposes. This duality allows system designers to reason explicitly about both desired and undesired behaviors within the same modeling framework.

In UML diagrams, misuse cases are depicted as black ovals labelled with malicious actions (e.g., 'Exploit SQL Injection'). They connect to normal use cases through 'threatens' and 'mitigates' associations, illustrating the relationship between attacker goals, system vulnerabilities, and defense mechanisms (

Figure 1). The technique integrates security early in system design, bridging communication between developers, analysts, and stakeholders.

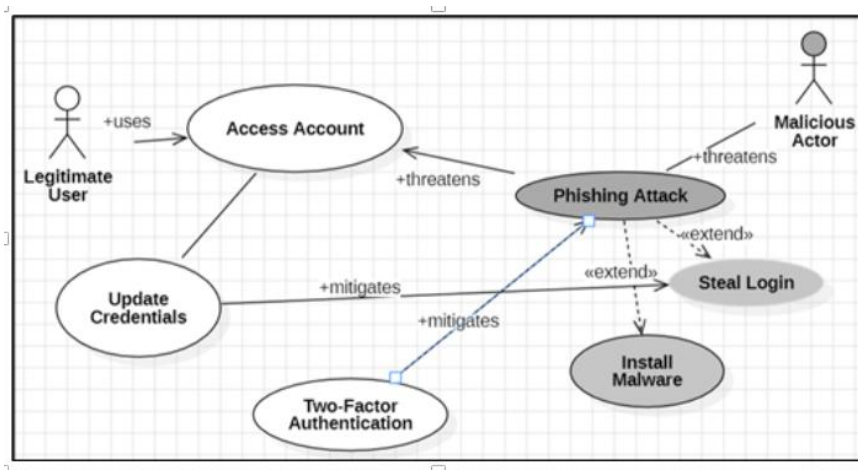


Figure 1:UML Use Case and Misuse Case diagram

Table 1 details the associations between Use Cases and Misuse Case in the above.

Table 1: Use Case and Misuse Case Associations

From	Association	To	Explanation
Phishing Attack	threatens	Access Account	The attacker tries to compromise login functionality
Two-Factor Authentication	mitigates	Phishing Attack	Adds an extra defense layer
Update Credentials	mitigates	Steal Login Credentials	Reduces long-term risk after a phishing attempt
Phishing Attack	extends	Steal Login Credentials	Credential theft is a sub-goal
Phishing Attack	extends	Install Malware	The attacker may trick the user into installing malicious software

Despite its strengths, traditional misuse case modeling often lacks grounding in empirical adversary data. This study enhances misuse case modeling by integrating it with the MITRE ATT&CK framework, aligning modelled threats with observed attacker behaviours. For example, annotating misuse cases with ATT&CK identifiers (e.g., T1566.001) provides traceability and validation based on real-world intelligence.

2.2. Threat Modeling Frameworks

Traditional threat modeling frameworks—such as STRIDE, DREAD, and PASTA—focus on identifying threats, vulnerabilities, and mitigations systematically. However, they often lack connections to threat intelligence. Shevchenko et al. (2018) emphasized that integrating operational data sources like ATT&CK into conceptual modeling frameworks enhances realism and detection coverage.

2.3. MITRE ATT&CK Framework

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework is a structured knowledge base that categorizes adversarial behaviors observed in real-world cyberattacks (MITRE Corporation, 2025). Developed by the MITRE Corporation, ATT&CK organizes adversarial actions into a hierarchical model of tactics, techniques, and procedures (TTPs).

Each technique in ATT&CK is associated with specific mitigations and detection guidance, allowing practitioners to translate abstract adversary behavior into actionable defensive measures (Strom et al., 2018). Mitigations (noted Mxxxx, e.g., M1043 - Credential Access Protection) represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. The framework is organized into multiple domain matrices—Enterprise, Mobile, and Industrial Control Systems (ICS)—ensuring applicability across Information Technology(IT), Operational Technology (OT), and cloud environments.

In practice, ATT&CK serves as a common reference model for cyber threat intelligence (CTI), detection engineering, red teaming, and security architecture. It facilitates standardized communication of threat behaviours, supports adversary emulation, and helps identify defensive coverage gaps (Roy et al., 2023). Moreover, ATT&CK's empirical foundation makes it particularly valuable for integrating threat intelligence into design-phase threat modeling.

The MITRE ATT&CK framework has become a global standard for classifying adversarial tactics, techniques, and procedures (TTPs) based on real-world observations (MITRE Corporation, 2025). It is widely adopted by Security Operations Centers (SOCs), red teams, and cyber threat intelligence (CTI) analysts. ATT&CK's structured representation of adversary behaviour has made it a cornerstone in operational cybersecurity, but its application during the design phase of systems—particularly in requirements and threat modeling—remains limited (Roy et al., 2023).

Besides the MITRE ATT&CK framework, MITRE has developed a tool, called **MITRE ATT&CK Navigator**, used to facilitate the exploration and visualization of adversarial tactics and techniques defined within the MITRE ATT&CK framework. It is an open-source web application that provides an interactive matrix interface that allows analysts, threat modelers, and defenders to annotate, color-code, and prioritize ATT&CK techniques according to their relevance, detection status, or mitigation coverage. Navigator supports the creation and sharing of

layer files (.json) that capture an organization’s defensive posture, threat assessments, or red-team scenarios.

Within the context of this research, the MITRE ATT&CK framework provides a taxonomy to enrich misuse case modeling. By linking misuse cases to ATT&CK techniques and mitigations, security analysts can trace system-level threats to real-world adversarial tactics, bridging the gap between conceptual threat modeling and intelligence-driven defence (Xiong et al., 2021).

The scope of this work is limited to the **Enterprise domain**.

2.4. ATT&CK-Driven Threat Modeling

Recent work (Xiong et al., 2021; Roy et al., 2023) has explored how ATT&CK can enhance system design and simulation. However, few methodologies explicitly integrate ATT&CK within UML-based modeling environments. This research closes that gap by providing a repeatable mapping method from misuse cases to ATT&CK techniques and mitigations.

3. METHODOLOGY

This section presents the proposed methodology for integrating UML misuse-case modeling with the MITRE ATT&CK framework. The objective is to ensure that each design-time threat is grounded in empirically observed adversarial behavior while maintaining traceability between system requirements, misuse cases, ATT&CK techniques, and defensive controls.

3.1. Methodological Overview

The methodology consists of seven sequential steps (Table 2) that combine security engineering principles with cyber threat intelligence. The process is adapted from Sindre and Opdahl (2005) and extended to incorporate the MITRE ATT&CK taxonomy.

Table 2: Methodology

Step	Description
1. Identify System Functions	List all primary use cases or system functionalities that may be targeted by attackers (e.g., login, data upload, file access).
2. Define Misuse Cases	For each system function, identify potential misuse cases (e.g., SQL injection, phishing, privilege escalation) that could compromise it.
3. Link to MITRE ATT&CK Techniques	Map each misuse case to one or more relevant MITRE ATT&CK techniques (TIDs). Use MITRE’s ATT&CK Navigator or the ATT&CK website for reference.
4. Describe Potential Impact	Describe what happens if the misuse case is successful (e.g., data breach, unauthorized access, service disruption).
5. Identify Mitigations	List mitigations from the MITRE ATT&CK framework (MIDs) or your own security controls that address this attack.
6. Assign Detection & Monitoring Controls	Link misuse cases to detection strategies, logs, or SIEM rules that can detect the ATT&CK technique in action.
7. Review and Update Regularly	Continuously review mappings as system functionality, threat landscape, or ATT&CK framework evolves.

This process creates traceability between conceptual system models and empirical adversary behavior data, aligning design decisions with recognized attack vectors and defensive measures.

3.2. Mapping Process

Each misuse case is annotated with its corresponding ATT&CK tactic and technique. For example (**Error! Reference source not found.**), the misuse case Phishing Attack is mapped to T1566.002 – Spearphishing Link under the Initial Access tactic. Relevant mitigations, such as M1031 – Network Intrusion Prevention, are associated with this misuse case. A traceability matrix connects misuse cases, ATT&CK techniques, mitigations, and detection mechanisms, forming the core of the proposed framework.

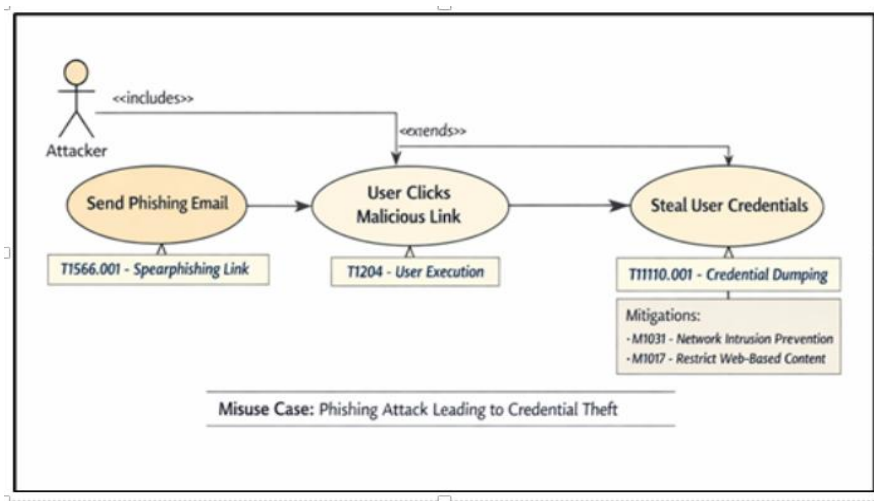


Figure 2: Mapping UML - ATT&CK

The following table visually represents how the Phishing Attack misuse case is mapped to MITRE ATT&CK techniques and mitigations coverage status:

Using the the MITRE ATT&CK matrix, we have the following view:

Table 3: ATT&CK matrix

Tactic	Technique	Coverage
Initial Access	T1566.002 – Spearphishing Link	● High Risk / Not Detected
Execution	T1204.002 – User Execution	● Partially Detected
Credential Access	T1539 – Steal Web Session Cookie	● Partially Detected
Mitigation Layer	M1032 – Multi-Factor Authentication	● Mitigated
Mitigation Layer	M1041 – Encrypt Sensitive Information	● Mitigated

Legend:

- **High Risk** — Techniques not yet detected (e.g., *T1566.001 Spearphishing Link*)
- **Partial Detection** — Techniques with some monitoring in place

- **Mitigated** — Techniques countered through defensive controls (e.g., MFA, encryption)

Implementation relies on UML tools like Enterprise Architect and ATT&CK Navigator (Ref:[5]) that can be complemented by Excel-based mapping templates. This setup enables integration within DevSecOps workflows and continuous assurance environments.

MITRE Navigator becomes a **bridge between UML misuse cases and operational threat intelligence** — you visualize the same attacks your misuse cases model, but in a structured, intelligence-driven way.

4. EXAMPLE AND DISCUSSION

To illustrate the proposed framework, a case study focusing on the *User Authentication* function was developed and a simplified phishing-based scenario demonstrates the integration process. Table 4 presents a subset of the resulting mapping between system functions, misuse cases, and ATT&CK techniques.

4.1. Scenario

A legitimate user attempts to access an account (*Access Account* use case), while an attacker launches a phishing campaign (Phishing Attack misuse case). The attack aims to steal user credentials (Steal Login Credentials misuse case). The system counteracts this threat with mitigation mechanisms such as Two-Factor Authentication and Email Filtering. These relationships form the foundation for mapping misuse cases to ATT&CK techniques and mitigations.

Table 4: Detailed Misuse Cases and MITRE ATT&CK Techniques

System Function	Misuse Case	ATT&CK Technique	Tactic	Impact	Mitigation
User Authentication	Phishing for User Credentials	T1566.002 - Spearphishing Link	Initial Access	Credential theft	M1017, M1031
Application Login	Brute-force attack	T1110.001 - Password Guessing	Credential Access	Unauthorized access	M1027, M1051
Server Console	Remote PowerShell execution	T1059.001 - PowerShell	Execution	Remote code execution	M1050, M1042

The full list of attributes (one row) includes [*System Function, Misuse Case Description, MITRE ATT&CK Technique ID (Txxx), Technique Name, Tactic (Phase), Potential Impact, Mitigations (Mxxx), Detection/Monitoring, Responsible Team, Risk Level (High/Med/Low)*].

NB: The complete table, with all attributes is as follows (Figure 3):

System Function	Misuse Case Description	MITRE ATT&CK Technique ID	Technique Name	Tactic (Phase)	Potential Impact	Mitigations (Mxxxx)	Detection/Monitoring	Responsible Team	Risk Level (High/Med/Low)
User Authentication	Attacker sends phishing email to obtain user credentials.	T1566.001	Phishing: Spearphishing	Initial Access	Compromise of user credentials,	M1017 - Restrict Web-Based Content; M1031 - Network Intrusion Prevention	Monitor email gateway logs for suspicious links and user clicks.	Security Operations Center (SOC)	High
Application Login	Attacker brute-forces user credentials using automated tools.	T1110.001	Brute Force: Password Guessing	Credential Access	Unauthorized access to application with valid user credentials.	M1027 - Password Policies; M1051 - Data Loss Prevention	Monitor failed login attempts and unusual login patterns in logs.	Application Security	Medium
Server Management Console	Attacker executes malicious PowerShell commands remotely.	T1059.001	Command and Scripting Interpreter: PowerShell	Execution	Remote code execution on critical systems, potential data	M1050 - Exploit Protection; M1042 - Disable or Remove Feature or Program	Monitor PowerShell execution logs and command-line arguments.	Infrastructure Security	High

Figure 3: Full picture (Attribute)

Integrating misuse case modeling with the MITRE ATT&CK framework represents a significant step toward unifying design-level threat modeling with operational threat intelligence.

4.2. MITRE ATT&CK Workflow Integration

A workflow diagram based on a phishing-driven attack scenario was developed to demonstrate the alignment between misuse-case modeling and the MITRE ATT&CK framework. The attack begins with T1566.002 – Spearphishing Link, in which the attacker delivers a malicious hyperlink via email. Upon user interaction, the workflow progresses to T1204.002 – User Execution, followed by T1539 – Steal Web Session Cookie, enabling the attacker to hijack authenticated sessions.

Each attack phase is associated with relevant ATT&CK mitigations, such as M1031 – Network Intrusion Prevention, M1042 – Disable or Restrict Script Execution, and M1032 – Multi-Factor Authentication.

These mitigations correspond directly to defensive misuse cases, enabling continuous traceability from design-time modeling to operational defense mechanisms.

This integration bridges conceptual threat modeling with empirical threat intelligence, allowing security architects to validate their system defenses quantitatively using ATT&CK coverage and the ATT&CK Navigator.

The workflow begins with the Initial Access tactic, represented by T1566.002 – Phishing: Spearphishing Link, where an attacker sends a fraudulent email containing a malicious hyperlink. Upon user interaction, this leads to T1204 – User Execution: Malicious File or Script, where the victim executes a payload, either by opening an infected document or running embedded scripts. Once executed, the attacker may escalate to T1539 – Steal Web Session Cookie, capturing authentication tokens or session identifier.

Each phase in the workflow is paired with one or more ATT&CK Mitigations (Mxxxx), such as:

- M1031 – Network Intrusion Prevention, to detect or block malicious URLs and attachments.
- M1042 – Disable or Restrict Script Execution, limiting unauthorized code execution.
- M1032 – Multi-Factor Authentication (MFA), reducing the impact of credential compromise.

These mitigations correspond directly to **security use cases** in the misuse case model, such as Two-Factor Authentication or Secure Login Validation. The integration demonstrates how real-

world ATT&CK techniques (TIDs) can be linked to UML misuse cases to provide a continuous traceability path — from design-time modeling through operational defence implementation.

This integration bridges conceptual threat modeling with empirical threat intelligence, enabling security architects to quantitatively validate system defences using ATT&CK coverage. It also supports the use of the MITRE ATT&CK Navigator for attack surface visualization and detection engineering, ensuring that mitigation strategies are aligned with known adversarial behaviors. (Figure 4)

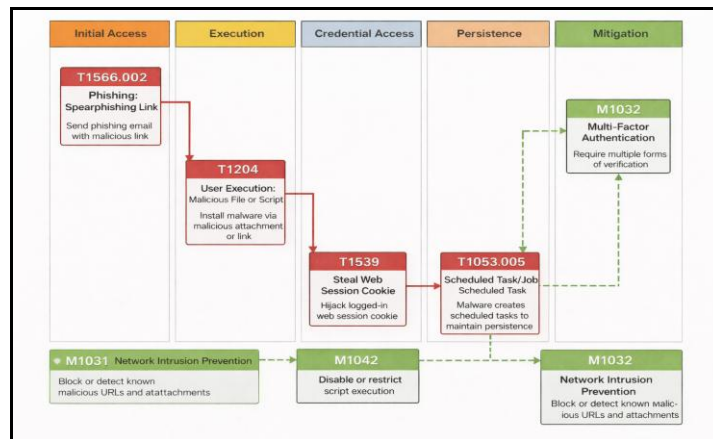


Figure 4: MITRE ATT&CK Navigator

The approach provides a traceable, intelligence-driven enhancement to traditional misuse case modeling. Where prior work emphasized conceptual modeling, the proposed framework operationalizes design artifacts with ATT&CK’s empirical adversary data, improving relevance and verifiability.

Practically, the methodology supports:

- Enhanced situational awareness through ATT&CK-informed threats.
- Cross-disciplinary communication via standardized terminology.
- Quantifiable defense validation by mapping mitigations to ATT&CK coverage.

Further details on MITRE frameworks can be found in the Reference [2], [3] and [4].

5. LIMITATIONS AND FUTURE WORK

Despite the structured methodology proposed, several limitations remain. The current integration between misuse case modeling and the MITRE ATT&CK framework is primarily conceptual, relying on manual mapping between UML elements and ATT&CK techniques. This dependency introduces subjectivity and potential inconsistencies across analysts.

Furthermore, the case study focuses on a phishing-based scenario; broader validation across diverse domains (e.g., IoT, cloud-native, or industrial control environments) remains necessary. Finally, automation and tool support for maintaining mappings between model elements and ATT&CK datasets are still limited.

Future research should explore semi-automated toolchains linking UML modeling environments, including the “Special Use Case” concept (Kabasele Tenday, 2010), with ATT&CK and CAPEC repositories. Empirical evaluations should compare this approach to existing methods like STRIDE and PASTA. Integrating AI-driven threat reasoning and real-time intelligence

enrichment could enable dynamic model evolution, supporting continuous threat-informed design.

6. CONCLUSION

This paper presented a unified framework that bridges UML misuse case modeling and the MITRE ATT&CK framework to achieve threat-informed system design. By systematically linking misuse cases to ATT&CK techniques and mitigations, the approach ensures that conceptual design models remain grounded in real-world adversarial behavior. The case study demonstrated how this methodology enhances traceability, visibility, and defensive consistency in early system development. Future work aims to extend this integration toward automation and validation across additional domains.

REFERENCES

- [1] Sindre, G., & Opdahl, A. L.(2005) Eliciting security requirements by misuse cases. *Requirement Engineering* 10(1), 34-44.
- [2] MITRE Corporation. (2025). MITRE ATT&CK Framework. Retrieved from <https://attack.mitre.org/>
- [3] MITRE_Mitigation Corporation.(2025) Retrieved from <https://attack.mitre.org/mitigations/enterprise/>.
- [4] MITRE_Tactics, (2025) Retrieved from <https://attack.mitre.org/tactics/enterprise/>.
- [5] MITRE_Navigator Corporation. (2025). Retrieved from <https://mitre-attack.github.io/attack-navigator/>.
- [6] Alexander, I. (2003), Misuse Cases: Use Cases with Hostile Intent. *IEEE Software*, 20(1), 58–66.
- [7] Shostack, A. (2020) *Threat modeling: Designing for security*. Wiley.
- [8] Shevchenko, N., et al. (2018).*Threat Modeling: A Summary of Available Methods*. Software Engineering Institute, Carnegie Mellon University.
- [9] Ponsard, C., & Grandclaudon, J. (2019). Bridging Model-Based Security Engineering and Threat Intelligence: Application to MITRE ATT&CK. *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES)*.
- [10] Roy, S., Panaousis, E., & Liu, W. SoK: (2023). The MITRE ATT&CK Framework in Cybersecurity Research and Practice. University of Surrey. Retrieved from <https://www.manospanaousis.com/files/pdf/papers/roy2023sok.pdf>.
- [11] Xiong, W., Lagerström, R., & Franke, U. An ATT&CK-based Threat Modeling Language for Model-Driven Security Analysis. *Software and Systems Modeling*, 21(3), (2021). 957–974. <https://doi.org/10.1007/s10270-021-00898-7>
- [12] Jean-Marie Kabasele Tenday. Using Special Use Cases for Security in the Software Development Life Cycle; (2010),Y. Chung and M. Yung (Eds.): WISA 2010, LNCS 6513, pp. 122–134, Jeju Island, Korea.

AUTHORS

Jean-Marie Kabasele Tenday holds a Ph. D in Computing Engineering from the Polytechnic School of Louvain, University of Louvain, Belgium. He works as Information System Security Expert, IT/OT security researcher and Professor in computer science for universities.

