Factsheet 05: Usefullness of AttackDefense Framework (ADF)

Introduction to ADF

The **AttackDefense Framework (ADF)** is a novel approach to **Threat Modeling (TM),** focusing on complex, multi-layered systems often overlooked by traditional TM methods. Developed in response to the limitations of current TM data models, ADF offers a robust and flexible data model to support the analysis and management of threats across a wide array of hardware, firmware, and software systems. This factsheet is based on the findings of the following paper: *"AttackDefense Framework (ADF): Enhancing IoT Devices and Lifecycles Threat Modeling" (Sacchetti, et al., 2024) published in the ACM Transactions on Embedded Computing Systems (TECS).*

Why is ADF needed?

Traditional threat modeling models and tools struggle to capture the complexity of embedded devices and systems spanning both hardware and low-level software. They often lack the capability to fully model device lifecycles or manage security-privacy tradeoffs - critical elements for effective TM in modern, multi-layered systems. Traditional models are frequently designed with specific use cases, such as software security or data privacy, which limits their adaptability to IoT scenarios, including low-level software, communications, and hardware threats.

ADF addresses these limitations by introducing a flexible data model structured around AD (Attack-Defense) objects. These modular building blocks allow ADF to represent heterogeneous and complex threats across different domains, enabling more adaptable threat modeling that accounts for device lifecycles and security-privacy tradeoffs.

The following graphic provides a high-level overview of the Attack Defense Framework and its integration with the threat modeling process. Each stage of the threat modeling process – *system modeling, threat identification, risk scoring, and defense planning* – is supported by ADF's tools, which enable the creation, validation, and organization of threat data.

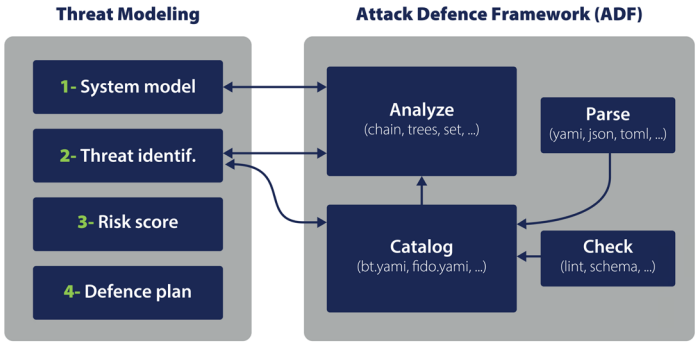

Figure 1: ADF high-Level Overview

Key Components of ADF

The AttackDefense Framework is built on a set of foundational components designed to enable effective and flexible threat modeling. These components support a systematic approach to identifying, representing, and mitigating security risks, specifically tailored for complex systems that involve multiple layers, such as hardware, firmware, and embedded software. At the heart of ADF are AD objects, modular building blocks that represent individual threats or defenses. AD objects allow for dynamic combinations, enabling users to construct adaptable and detailed threat models suited to diverse security landscapes. These objects can be visualized and organized in various ways – such as through chains, sets, or word clouds – offering comprehensive views of relationships and dependencies among threats.

To further support its functionality, ADF includes a robust suite of Toolkit Modules. These four modules – Catalog, Parse, Check, and Analyze – are specifically designed to facilitate the creation, validation, and analysis of AD objects. Together, these components form the backbone of ADF, streamlining the threat modeling process and equipping users with the tools needed to manage and understand complex security challenges effectively.

Evaluating ADF's Effectiveness

The effectiveness of the AttackDefense Framework was demonstrated through extensive testing on a crypto wallet's lifecycle, involving seven expert groups from academia and industry. Each group applied ADF to unique threat classes, including side-channel attacks, fault injection, speculative execution, and Bluetooth protocol threats. The thorough evaluation produced 175 high-quality components that effectively addressed a wide range of security challenges, confirming ADF's ability to handle complex threats and proving its value as a reliable tool for modern security analysis.

ADF's Unique Contributions – an Overview

1. **Broad Applicability:** ADF is suitable for hardware, firmware, and embedded systems, extending TM capabilities to multi-layered device architectures.
2. **Lifecycle Modeling:** ADF represents complete device lifecycles, supporting a comprehensive approach to security.
3. **Automation and Efficiency:** ADF's toolkit automates the creation and management of threat models, enhancing productivity by reducing manual efforts.
4. **Enhanced Visualization:** Visualization tools (e.g., word clouds, trees) provide an intuitive understanding of threat structures and their interdependencies.

Real-World Impact

The AttackDefense Framework enables organizations to identify and address security threats spanning both hardware and software, model device lifecycle threats crucial for embedded systems and critical infrastructure and optimize security-privacy trade-offs for balanced decision-making. Its applications extend across industries such as IoT, financial technology, and automotive security, making it a valuable tool for advancing security practices in increasingly interconnected threat environments.

Figure 2: ADF's comprehensive coverage

Conclusion

ADF presents a versatile, robust, and comprehensive approach to modern Threat Modeling. Its adaptability, modular structure, and automation capabilities make it an invaluable tool for organizations looking to strengthen their security frameworks in complex, multi-layered systems.

Funded by the European Union

The ORSHIN project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101070008.