July Community Meetup

10:00

Automating Threat Modeling: Challenges and AI Solutions

July 24th | 11:00am ET

Hosted by:

Audrey Long
Sr. Software Engineer @ Microsoft

About the Community Meetup

- **Our Goal**
  Exchange real-world experience, share practical knowledge, validate ideas to improve our own practice.

- **Chatham House Rule**
  Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

- **New format:** Small group, facilitated discussion

Agenda

11:00	Welcome, intro, photo
11:05	Presentation
11:25	Small group discussion
11:45	Readout and insight sharing
11:55	Closing and announcement

Photo Time!

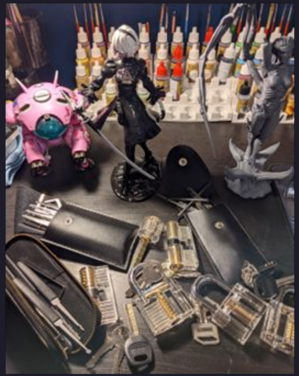
About me

I Love Cooking, Creating, and Learning

Women Techmakers

Google

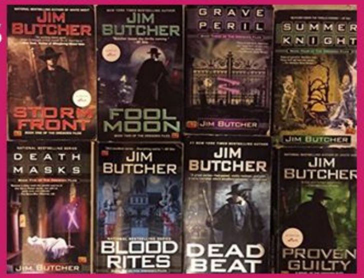
Digital Design
Ruby in Practice
Essential Scrum
User Stories Applied
Ruby
Exploring Raspberry Pi
Security in Computing
Cryptography Theory and Practice
Horstmann Big Java Early Objects
Starting Out with C++ From Control Structures through Objects
An Embedded Software Primer
Security Engineering A Guide to Building Dependable Distributed Systems



University of CINCINNATI

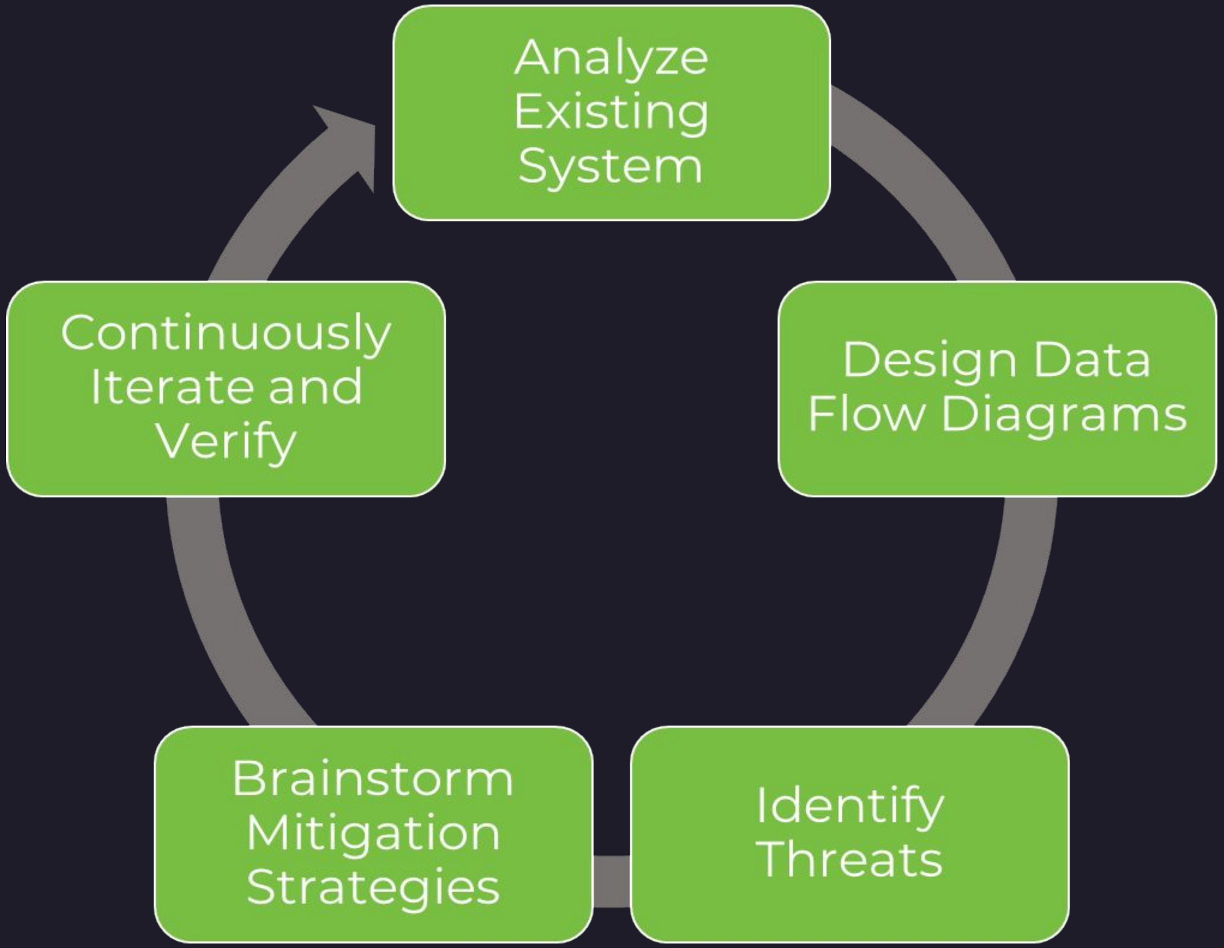
JOHNS HOPKINS UNIVERSITY

My Favorite Book Series



My Favorite Games

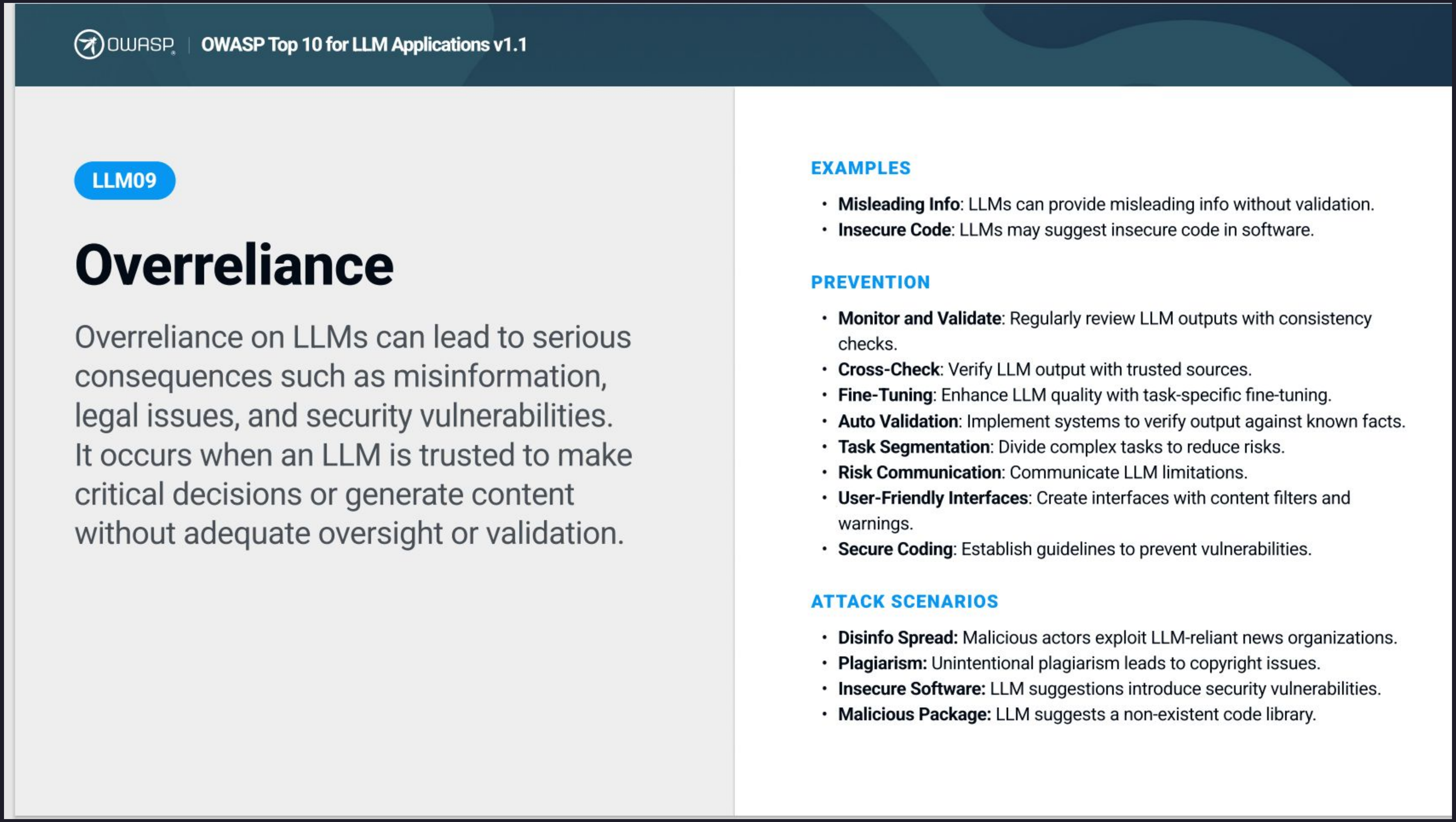
Basic Threat Modeling Algorithm


Analyze Existing System
Design Data Flow Diagrams
Identify Threats
Brainstorm Mitigation Strategies
Continuously Iterate and Verify

What Can We Automate?

- Analyze Existing System
- Design Data Flow Diagrams
- Identify Threats
- Create Countermeasures
- Continuously Iterate and Verify

Create Tools and Use AI Responsibly!



OWASP | OWASP Top 10 for LLM Applications v1.1

LLM09

Overreliance

Overreliance on LLMs can lead to serious consequences such as misinformation, legal issues, and security vulnerabilities. It occurs when an LLM is trusted to make critical decisions or generate content without adequate oversight or validation.

EXAMPLES

- **Misleading Info**: LLMs can provide misleading info without validation.
- **Insecure Code**: LLMs may suggest insecure code in software.

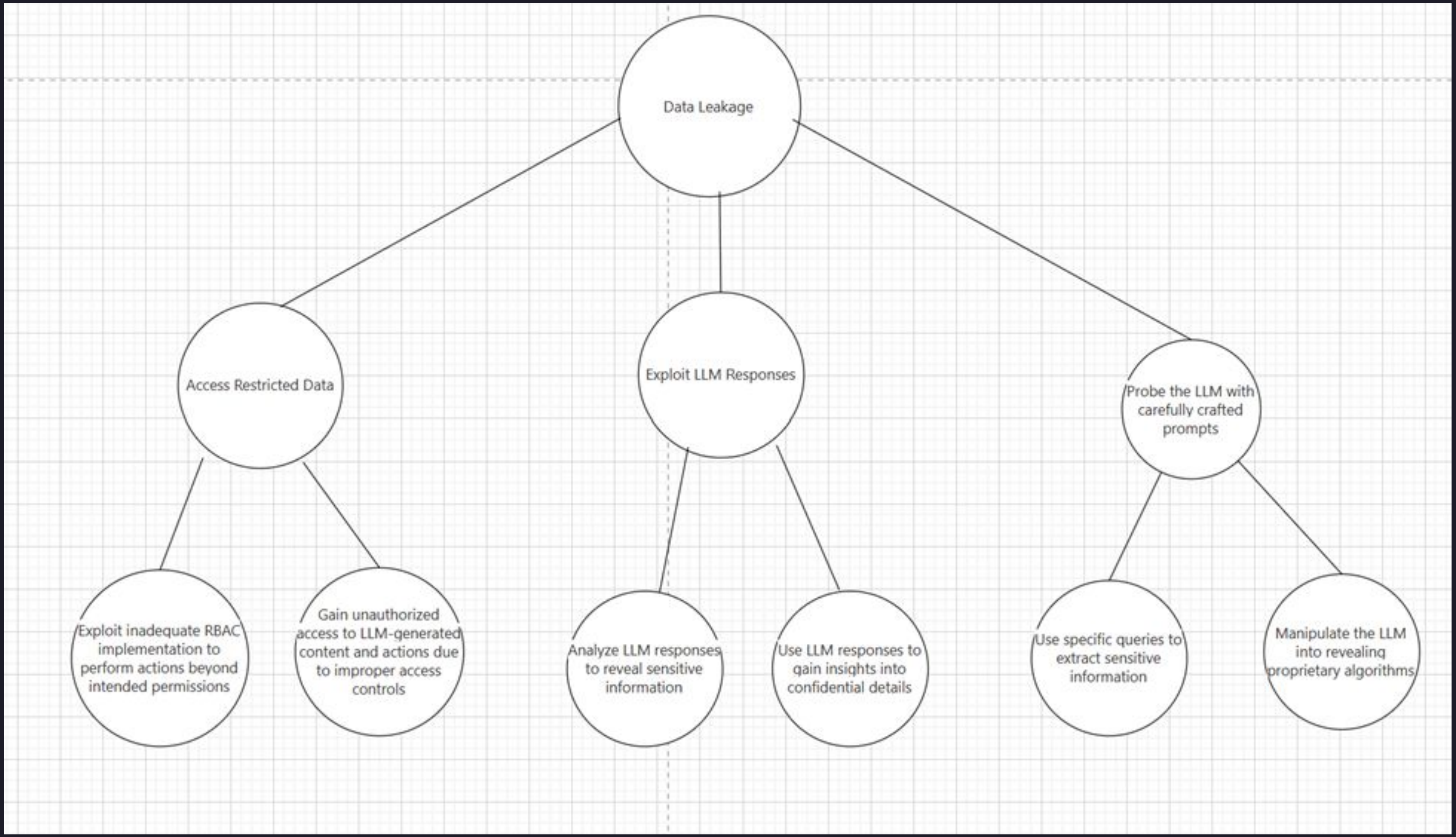
PREVENTION

- **Monitor and Validate**: Regularly review LLM outputs with consistency checks.
- **Cross-Check**: Verify LLM output with trusted sources.
- **Fine-Tuning**: Enhance LLM quality with task-specific fine-tuning.
- **Auto Validation**: Implement systems to verify output against known facts.
- **Task Segmentation**: Divide complex tasks to reduce risks.
- **Risk Communication**: Communicate LLM limitations.
- **User-Friendly Interfaces**: Create interfaces with content filters and warnings.
- **Secure Coding**: Establish guidelines to prevent vulnerabilities.

ATTACK SCENARIOS

- **Disinfo Spread:** Malicious actors exploit LLM-reliant news organizations.
- **Plagiarism:** Unintentional plagiarism leads to copyright issues.
- **Insecure Software:** LLM suggestions introduce security vulnerabilities.
- **Malicious Package:** LLM suggests a non-existent code library.

AI Attack Trees


Data Leakage
Access Restricted Data
Exploit LLM Responses
Probe the LLM with carefully crafted prompts
Exploit inadequate RBAC implementation to perform actions beyond intended permissions
Gain unauthorized access to LLM-generated content and actions due to improper access controls
Analyze LLM responses to reveal sensitive information
Use LLM responses to gain insights into confidential details
Use specific queries to extract sensitive information
Manipulate the LLM into revealing proprietary algorithms

Demos

1. How to use Azure’s OpenAI Studio to create Attack Trees
2. How to create Attack Tree tools with Azure OpenAI endpoint

Small group discussion

- **Question 1: What challenges do you face with automated threat modeling?**
- **Question 2: How have you used AI to support your threat modeling efforts?**

Insight Sharing

Summary of key highlights and top takeaways from each group

Next Meetup: “Meta Threat Modeling” (August 23rd, 2024)

- **Become a facilitator:** Sign up to become a facilitator and help guide the breakout sessions in our future meetups.
- **Join our speaker lineup:** Submit your talks to present at future meetups.
- **Follow us on LinkedIn @Threat Modeling Connect:** Events, content, updates, and more!