Cybersecurity Keynote

Standards and Performance Metrics for On Road Vehicle Workshop

September 6, 2023

Anuja Sonalker, Ph.D
STEER

Generative **AI**

In the context of On Road Vehicles

Generative AI uses ML models to generate **new and original** content based on inputs and training

Adversary **Upgrade**

In the context of On Road Vehicles

Hobby Hacker

Expert Researchers/System Professionals

Nation States and Organized Crime

Hobby **Hacker**

High motivation for personal gain

Limited financial resources

Limited skill set

Expert Researchers

Access to documentation, tools, networks

Motivation is for improvement

Competitors and Criminals

Financial motivation

Access to insider information, sophisticated tools

Nation States and **Terrorists**

Unlimited Financial Resources

Financial or ideological motivation

Access to sophisticated talent pool and tools

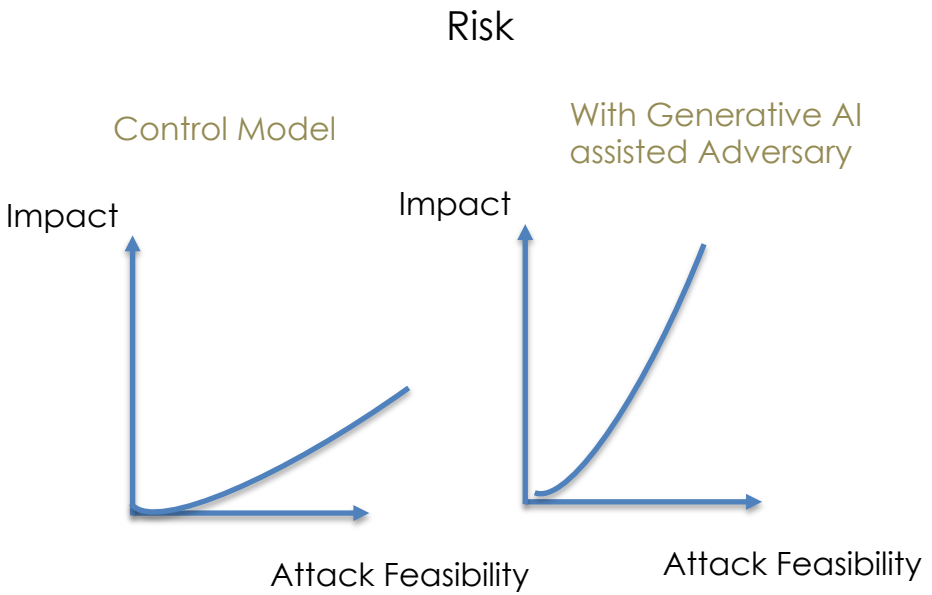
Risk Posture

In the context of On Road Vehicles

Threat Landscape

Attack Potential and Feasibility

Impact



Attack Feasibility

In the context of On Road Vehicles

Time

Expertise

Knowledge

Window of Opportunity

Equipment

Standards based approach to developing automotive systems

In the context of On Road Vehicles

Lockdown Levels of Risk

Apply Treatments Accordingly

Not Just an Engineering Concern

Risk Treatments Span Verticals

Approach

In the context of On Road Vehicles

Continuous monitoring of AI maturity

Measurement (Metrics) to assign tangibility

Blueprint for counter moves

Tactical Roadmap for execution of the blueprint

THANK YOU!