A Stackelberg Game Theory Approach to Mitigating Cyber Risk in Critical Railroad Infrastructure

Problem Statement and Goals

Problem Statement

The railroad industry is a part of critical infrastructure that provides essential transportation services such as enabling economic activity, supporting supply chains, and efficiently moving bulk materials. Within the industry, shortline railroads, responsible for last-mile delivery, are becoming increasingly susceptible to cyber attacks due to limited resources and concern.

Goal:

Provide actionable guidance for shortline railroads to efficiently allocate their resources to harden their defenses and comply with national cybersecurity mandates.

Approach

Apply Stackelberg Game Theory (a leader-follower game model where a defender commits to a strategy while attackers respond optimally).

Gather insights from literature reviews and conduct stakeholder interviews.

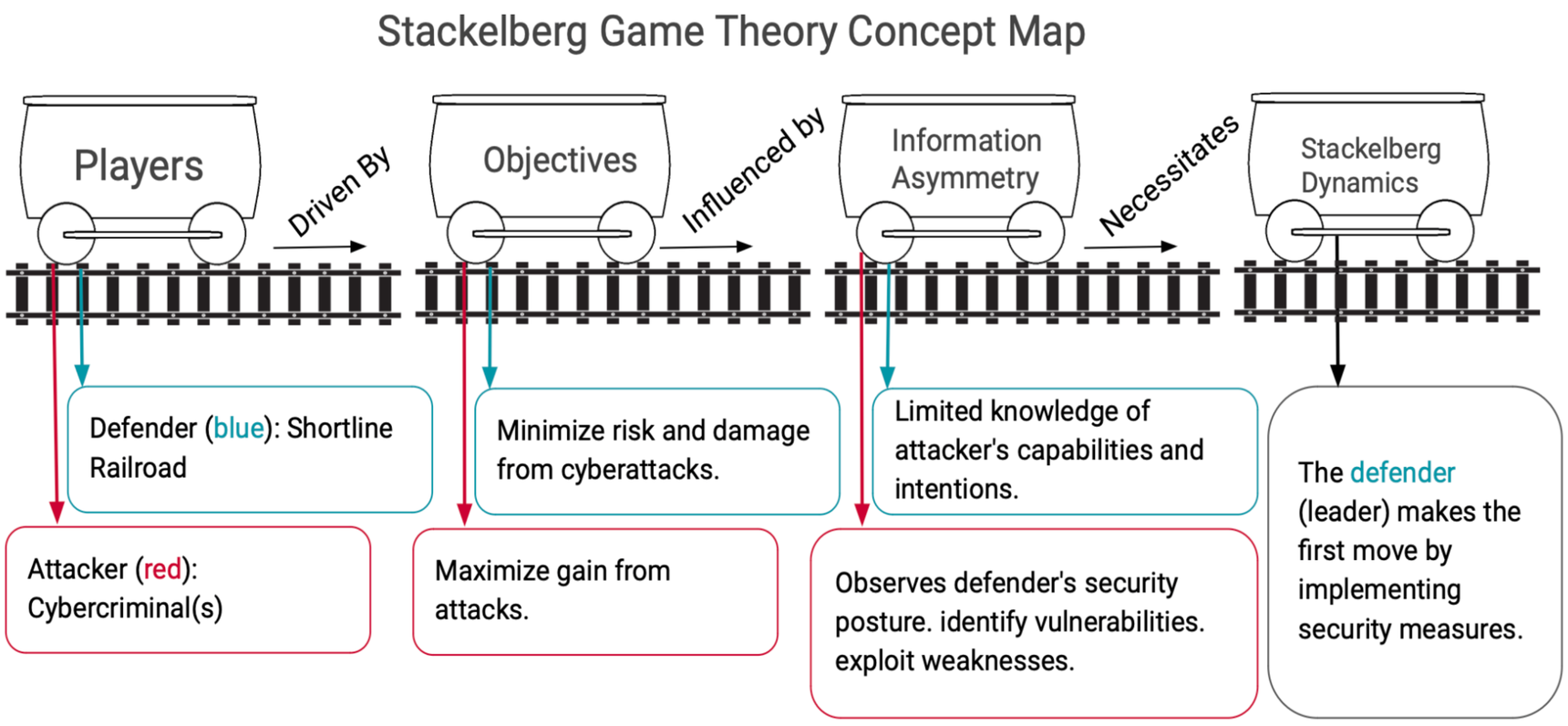
Model attacker-defender dynamics to pinpoint vulnerabilities and risk.

Quantify risks and identify mitigations based on real breach reports and evidence.

Suggest actionable steps that adhere to national mandate requirements.

Results

Outcome: A proof-of-concept tool that ranks cyber risk mitigations based on the organization's current cybersecurity posture and investment. It helps prioritize spending across systems that strengthen defense-in-depth protection while meeting regulatory requirements.



Future work: Provide the tool with a user interface and iterate on feedback from FRA and TSA stakeholders about applicability to shortline railroad organizations.

Jackie Hong
Rutgers University

RUTGERS THE STATE UNIVERSITY OF NEW JERSEY

A Stackelberg Game Theory Approach to Mitigating Cyber Risk in Critical Railroad Infrastructure

Abstract

Cybersecurity is a growing concern within the railroad industry as rail systems increasing rely on interconnected IT and OT systems responsible for safety, efficiency, and daily operations. Many railroad organizations face an elevated cyber risk exposure due to having limited resources such as budget, staff, and training allocated to their cybersecurity program. Cyber attacks have been demonstrated to disrupt operations which has national implications for passenger safety, public perception, supply chain disruption, and economic damage.

This project applies a Stackelberg game theory framework to analyze and mitigate cyber risk within critical railroad infrastructure with a particular focus on shortline railroads that often operate under limited resources. By modeling cybersecurity as a strategic interaction between defenders (railroad organization) and an attacker (cybercriminal), we capture attacker-defender dynamics and decision-making when investing resources. The results are informed through literature review, stakeholder interviews, and are grounded by real-world breach reports to prioritize the most exploited vulnerabilities and the most impactful risks to the organization and national security.

The outcome of this work is a proof-of-concept model for a tool for railroad organizations that helps them rank cybersecurity mitigations based on the organization's current security posture. The model encourages efficient allocation of resources by prioritizing controls that provide the greatest risk reduction based on our findings while adhering to defense-in-depth strategies and compliance with national cybersecurity mandates. This work offers actionable guidance for shortline railroads seeking to harden their systems against cyber threats.

Jackie Hong
Rutgers University

RUTGERS THE STATE UNIVERSITY OF NEW JERSEY