A Game theory Based Cybersecuity assessment model for advanced manufacturing systems

Zhejiang University
Zuoqi Tang
tangzq@zju.edu.cn

基于博弈论的先进制造系统的网络安全评估模型

Zhejiang University
Zuoqi Tang
tangzq@zju.edu.cn

Warm up Game

- Write down **your name** and a letter **"A"** or **"B"**

  Secretely on a **paper(hand)**

- We will pair you randomly with another student.
  - *If you write down **"A"** and your pair puts **"B"**,then you will get grade **A** and your pair gets **C.***
  - *If both you write down **"A",** then you both get rade **B-.***
  - *If you write down **"B"** and your pair puts **"A",** then you will get grade **C** and your pair gets **A.***
  - *If both you write Down **"B",**then you both get Grade **B+.***

Outlines

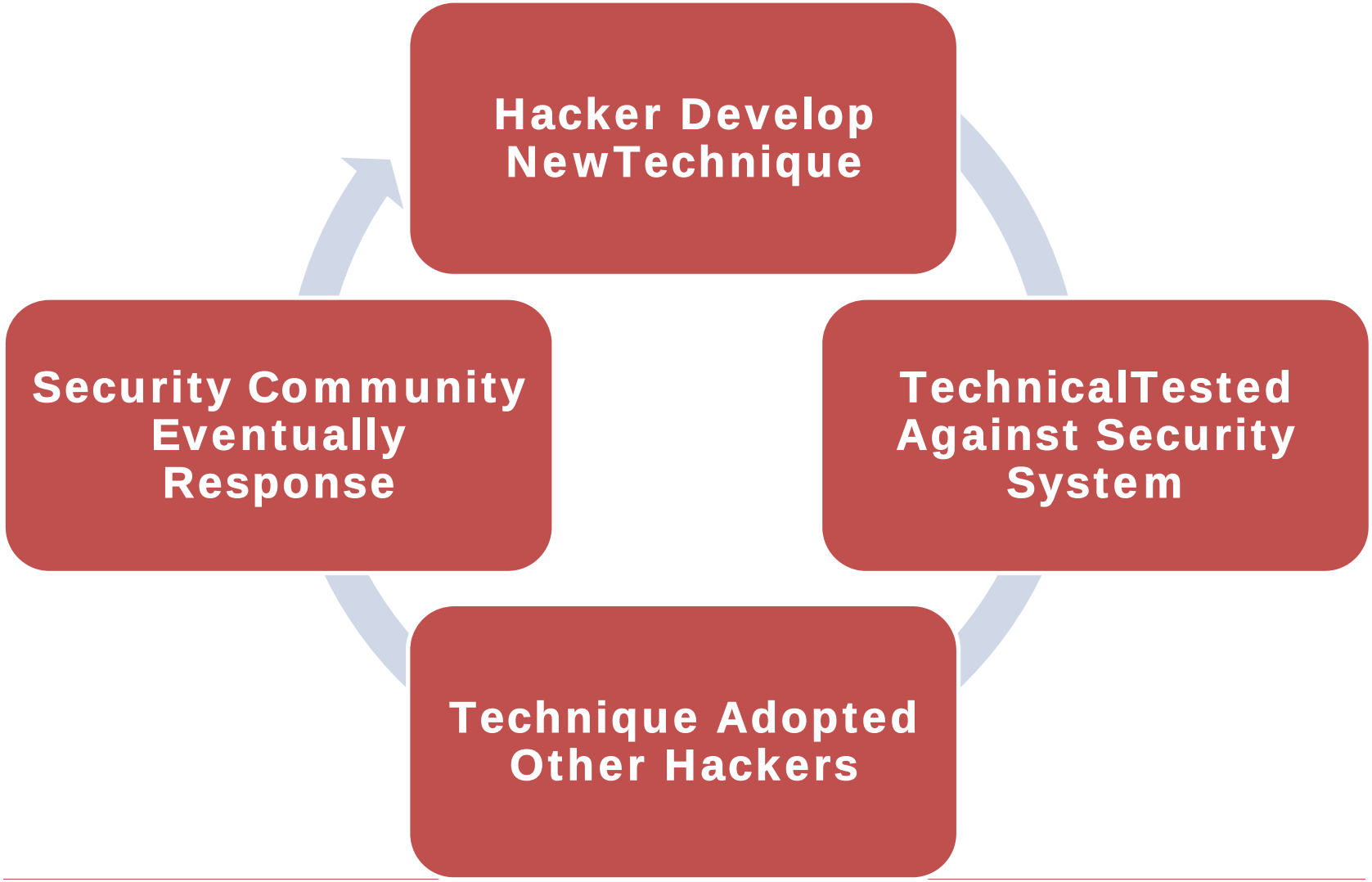
- Literature Review
  - Game Thoery
  - Cybersecuriy Assessment
- Modeling
- The Model Using Game Theoretical Methods
- Numerical Case Study
- Summary

大纲

- 背景知识
  - 博弈论
  - 网络安全评估
- 安全建模
  - 参考者
  - 策略空间
  - 效用函数
- 运用博弈理论方法对模型进行分析
- 案例

背景知识

背景知识-CyberSecurity



安全建模- Modeling

CyberSecurity Assessment Model

- Players
  - Attacker
  - Defender
- Action Sets
  - Defense mechanism
  - The action set for attacker
- Reward Function(Payoff matrix)
  - TheAttackers' movtivation
  - A reward and cost

Nomenclature- 符号与意义

π	Probability of attack
φ	Probability of defense
Γ	GameValue,Payoffmatrix
D	Set of strategies for the defense
A	Set of actions for attacker
n	Number of action types for attacker
m	Number of action types for strategies
E	Matrix of effectiveness
s	Cost of implementing and maintaining

Nomenclature- 符号与意义-cont.

S	Matrix of spending
G	Matrix of gain
p	Rate of the loss in production for each typye of attacks
P	Matrix of production lost
r	Cost of recovery from each typye of attacks
R	Matrix of cost of revovery
T	Total production

模型分析-Analyzing

Reward function(Payoff matrix)

$$\Gamma = \begin{bmatrix} \gamma_{11} & \cdots & \gamma_{1m} \\ \vdots & \ddots & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nm} \end{bmatrix}$$

Amount that attacker gains/lose

$$\gamma_{ij} = \underbrace{s_j - (s_i \times e_{ij})}_{\text{maintenance cost}} + \underbrace{T \times p_i \times (1 - e_{ij})}_{\text{cost of production loss}} + \underbrace{r_i \times (1 - e_{ij})}_{\text{cost of recovery}}$$

Effective matrix-经验值

$$E = \begin{array}{c} \\ a_1 \\ \vdots \\ a_n \end{array} \begin{array}{c} \begin{array}{ccc} d_1 & \cdots & d_m \end{array} \\ \begin{bmatrix} e_{11} & \cdots & e_{1m} \\ \vdots & \ddots & \vdots \\ e_{n1} & \cdots & e_{nm} \end{bmatrix} \end{array}$$

效用函数-Global utility/game value

$$U^* = \min_{\varphi} \max_{\pi} U_{ij}(\pi(a_i), \varphi(d_j), \gamma_{ij})$$

规划问题求解-Mixed strategy game

$$\min \sum_j \varphi_j$$

$$\begin{cases} \sum_j \gamma_{ij}\varphi_j \le 1 & (i=1,2,\dots n) \\ \varphi_j \ge 0 & (j=1,2,\dots m) \end{cases}$$

$$\min \sum_i \pi_i$$

$$\begin{cases} \sum_i \gamma_{ij}\pi_i \ge 1 & (i=1,2\dots,n) \\ \pi_i \ge 0 & (j=1,2\dots,m) \end{cases}$$

案例研究- Case Study

实验演示-Assume

$$s = \{3, 50, 10, 300, 0\}$$

$$p = \{0.5, 0.1, 0.7, 1\}$$

$$T = 1000$$

$$r = \{15, 20, 100, 300)$$

实验演示-Assume-Effectiveness Matrix

$$E = \begin{bmatrix} 1 & 0.1 & 0 & 0 & 0 \\ 0.98 & 0.5 & 0 & 0 & 0 \\ 0 & 0.3 & 0.98 & 0.8 & 0 \\ 0 & 0.92 & 0.7 & 0.98 & 0 \end{bmatrix}$$

实验演示-Payoff Matrix

$$\Gamma = \begin{bmatrix} 0 & 103.5 & 75 & 365 & 65 \\ 2.46 & 85 & 130 & 420 & 120 \\ 803 & 595 & 16.2 & 220 & 800 \\ 1303 & 108 & 393 & 32 & 1300 \end{bmatrix}$$

实验演示-Game Value-Result

Game Value：212.719

$$\pi = \{0, 0.35, 0.23, 0.41\}$$

$$\varphi = \{0, 0.21, 0.45, 0.32, 0\}$$

存在的问题与挑战

- 假设条件
  - 静态
  - 双人零和博弈
  - 完全信息
  - 理性
- 挑战
  - 动态
  - 多人（如RL中多Agent）
  - 不完全信息
  - 合作博弈、演化博弈

未来研究方向

- Game Theory + Computing=Algorithm Game
- Game Theory + AI(ML/RL)
- Game Theory + Game
- Game Theory + Mechanisms Design

Deep Reinforcement Learning

Thanks

Outcomes Matrix

You \ Your Pair	"A"	"B"
"A"	(B-,B-)	(A,C)
"B"	(C,A)	(B+,B+)