Game-Theoretic Simulation in Cyber Security

Agents

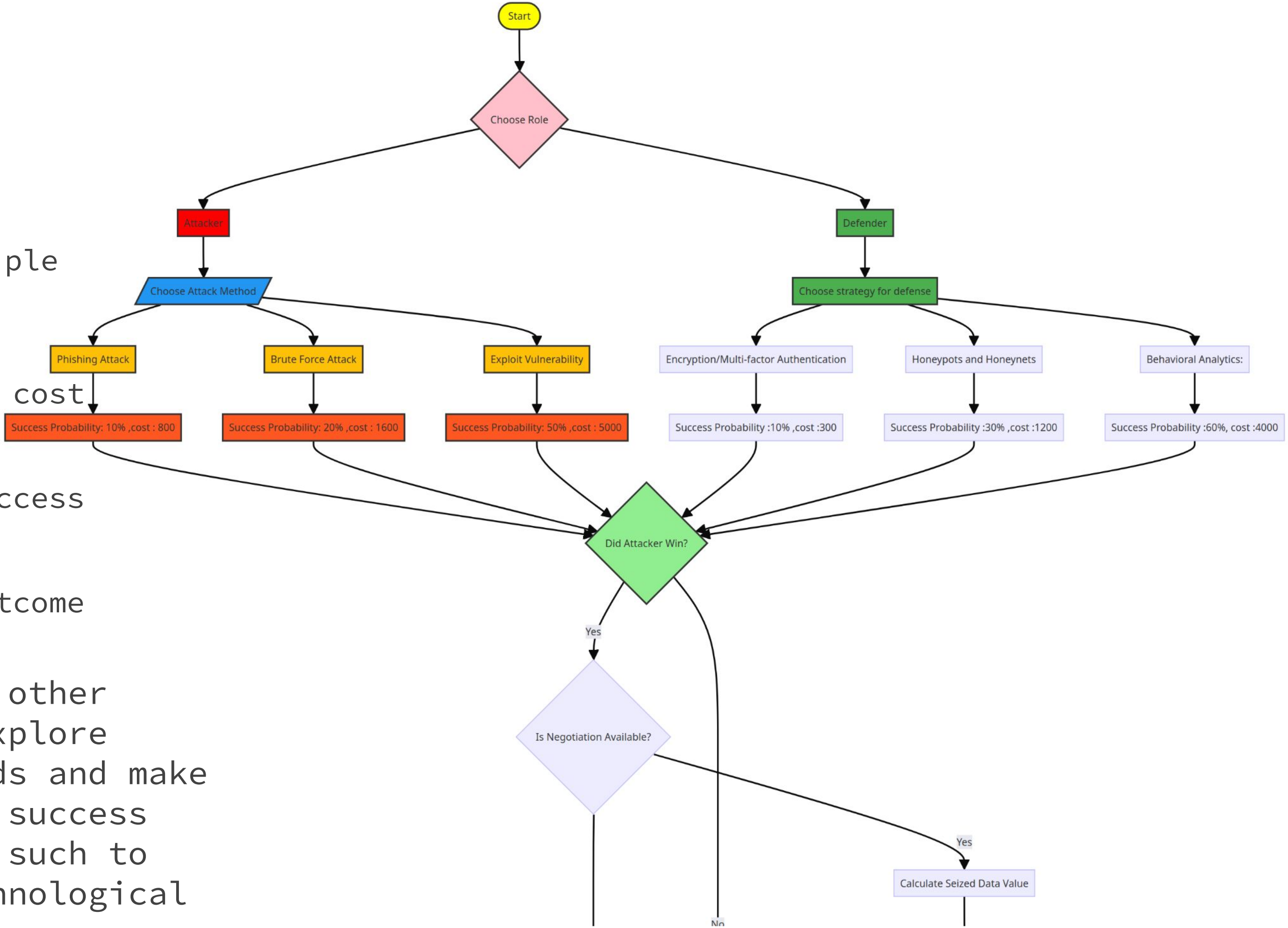
-Attacker

-Defender

At first we have various options available for Defenders as well as attackers.Each options are associated with payoffs and their costs

FlowChart - Engagement

- We can have Multiple Options for both Sides with varying cost and Probability of success choice Of either decides outcome of game
- We can also add other options as we explore different methods and make the methods and success rate dynamic as such to incorporate technological advancement



Start
Choose Role
Attacker
Defender
Choose Attack Method
Choose strategy for defense
Phishing Attack
Brute Force Attack
Exploit Vulnerability
Encryption/Multi-factor Authentication
Honeypots and Honeynets
Behavioral Analytics:
Success Probability: 10% ,cost : 800
Success Probability: 20% ,cost : 1600
Success Probability: 50% ,cost : 5000
Success Probability :10% ,cost :300
Success Probability :30% ,cost :1200
Success Probability :60%, cost :4000
Did Attacker Win?
Yes
Is Negotiation Available?
Yes
Calculate Seized Data Value
No

How Do we Handle Interaction between simultaneous attack Defense move

With varying amount of cost and probability in both sides. We will generate random numbers to simulate the outcome of the engagement.

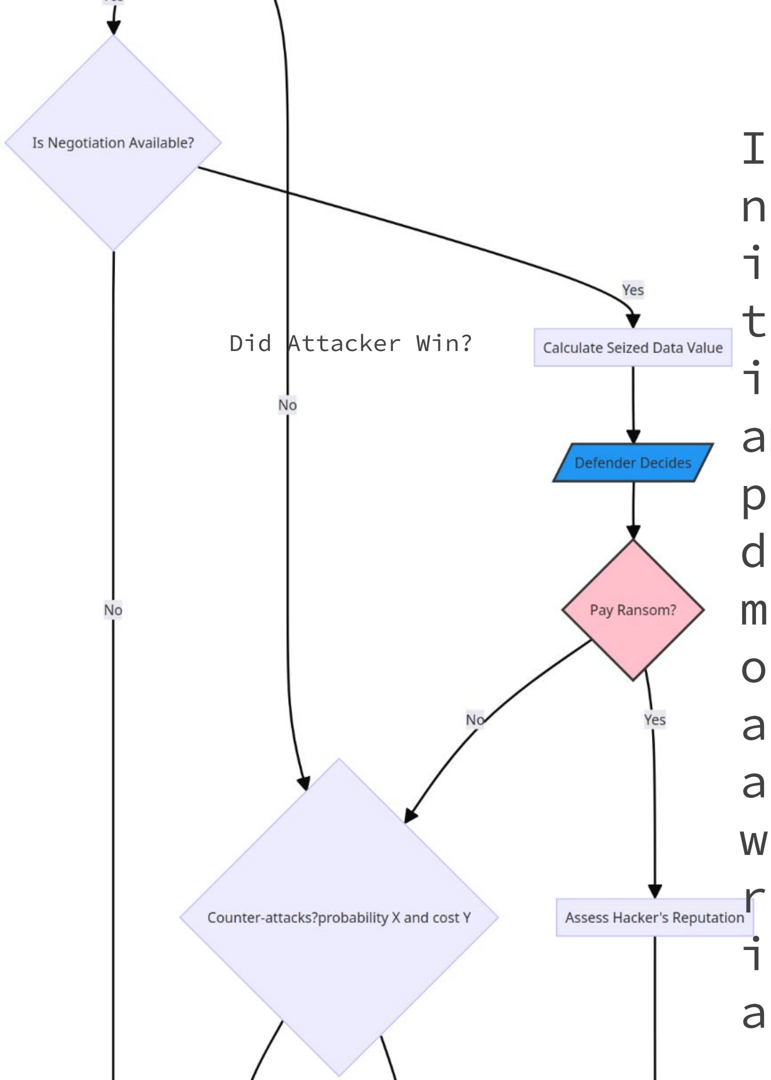
For example: If attacker uses an attack which succeeds 40% (P1)of time and defender defends its data with defense mechanism with reliability of 50%(P2) of time.

Outcome of successful attack = $P= \frac{40}{50+40} \% = 44.44\%$

So we can generate a random number between 0 and 10000 and check if its less than 4444 then we simulate the attack

Aftermath

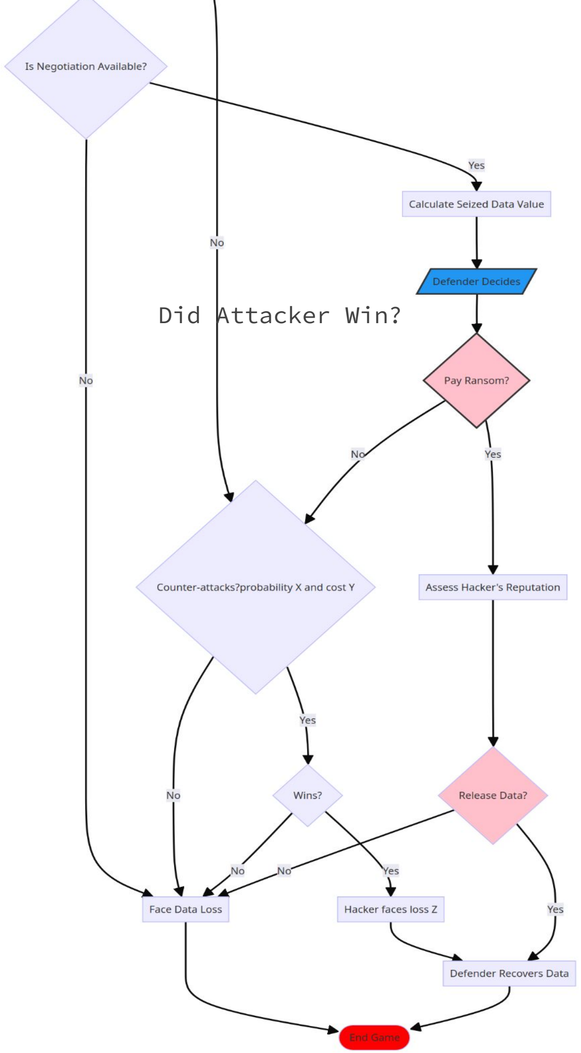
Then depending on success of attack ? There further hope for negotiation if possible , if the hacker is greedy for money then or defender being too desperate


Is Negotiation Available?
Yes
No
Did Attacker Win?
No
Calculate Seized Data Value
Defender Decides
Pay Ransom?
No
Yes
Counter-attacks?probability X and cost Y
Assess Hacker's Reputation

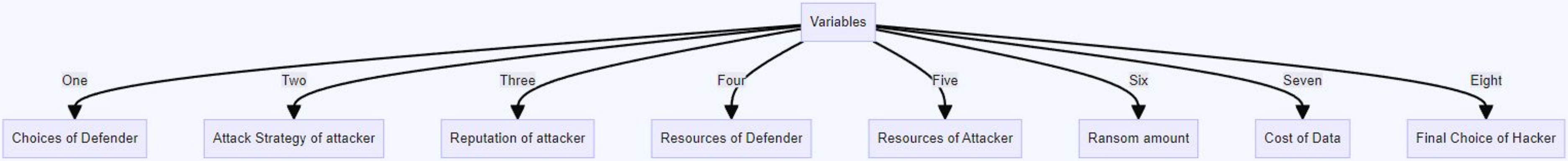
If negotiation is possible then there is Ransom amount to pay.Or the defender might outsmart and counter attack which is risky indeed with added cost

Outcome

Depending on Success of Counterattack/ payment of negotiation or failure from both sides results in respective results



Possible Variables



Variables

One

Two

Three

Four

Five

Six

Seven

Eight

Choices of Defender

Attack Strategy of attacker

Reputation of attacker

Resources of Defender

Resources of Attacker

Ransom amount

Cost of Data

Final Choice of Hacker

Final FlowCh

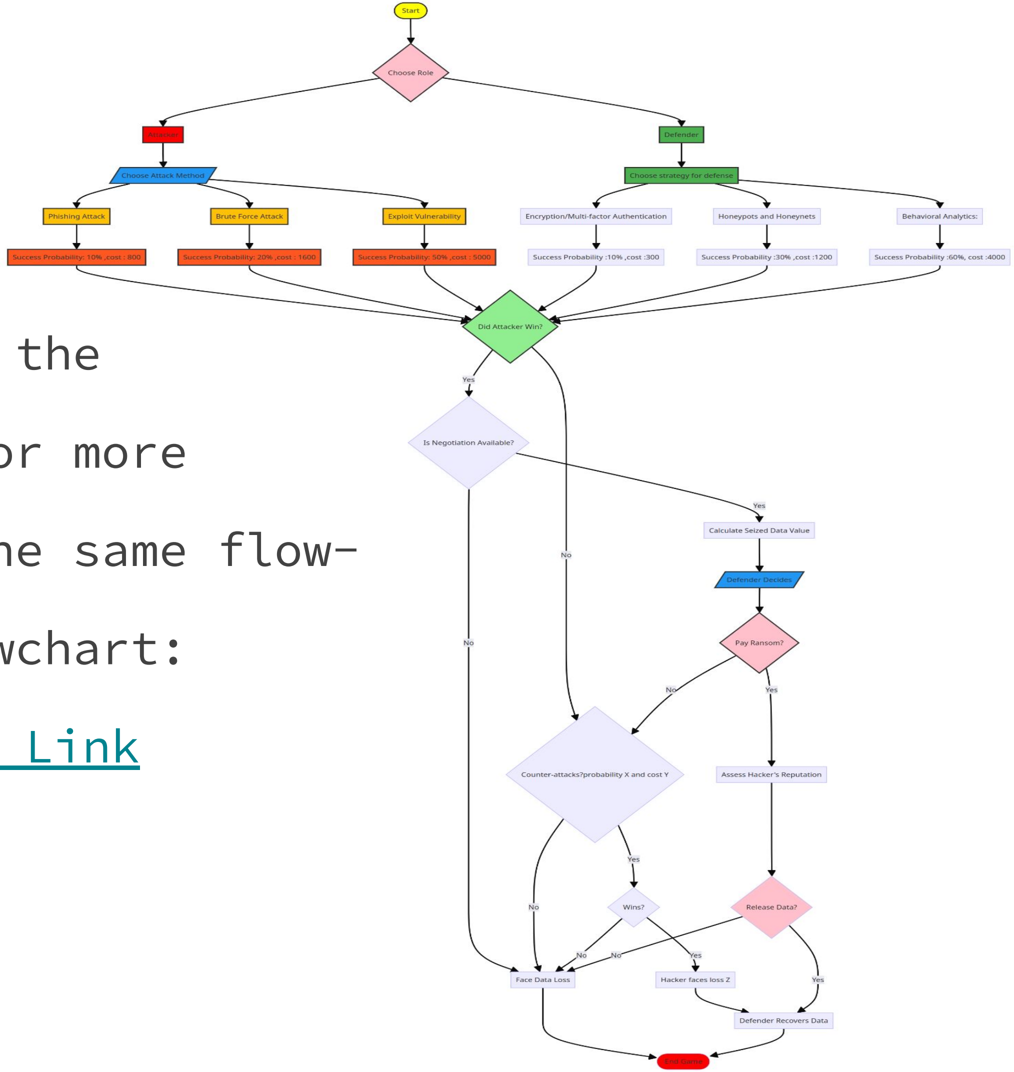
Kindly visit the

Link below for more

Clarity of the same flow-

Extended flowchart:

- FlowChart Link
- Backup


Start
Choose Role
Attacker
Defender
Choose Attack Method
Choose strategy for defense
Phishing Attack
Brute Force Attack
Exploit Vulnerability
Encryption/Multi-factor Authentication
Honeypots and Honeynets
Behavioral Analytics:
Success Probability: 10% ,cost : 800
Success Probability: 20% ,cost : 1600
Success Probability: 50% ,cost : 5000
Success Probability :10% ,cost :300
Success Probability :30% ,cost :1200
Success Probability :60%, cost :4000
Did Attacker Win?
Yes
Is Negotiation Available?
No
Yes
Calculate Seized Data Value
Defender Decides
No
Pay Ransom?
No
Yes
Counter-attacks?probability X and cost Y
Assess Hacker's Reputation
Yes
No
Wins?
Release Data?
No
No
Yes
Yes
Face Data Loss
Hacker faces loss Z
Defender Recovers Data
End Game

Thank You