Hypergames and Cybersecurity

Tonicha Crook
1915995@swansea.ac.uk

Swansea University

October 2022

UKRI CENTRE FOR DOCTORAL TRAINING IN ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND ADVANCED COMPUTING

Outline

1. Introduction

2. Background in Game Theory

3. Hypergames

4. Using Hypergames
    - Hyper-Nash Equilibrium
    - Stable Hyper-Nash Equilibrium

5. Applications in Cybersecurity

Introduction

Hypergames are a system comprised of a set of games with incomplete information.

Hypergames help find solutions to situations where there are miscommunications of events or strategies available.

Describing Games

Some key elements to describe a game:

1. The amount of players

Describing Games

Some key elements to describe a game:

1. The amount of players
2. Possible actions available to players

Describing Games

Some key elements to describe a game:

1. The amount of players
2. Possible actions available to players
3. A rule determining the outcome of every possible ending

Describing Games

Complete Information

Complete Information means the structure of the game and the payoffs/utility functions of the players are common knowledge.

Describing Games

Complete Information

Complete Information means the structure of the game and the payoffs/utility functions of the players are common knowledge.

Perfect Information

Perfect Information is when all players know every move that has been previously made.

Strategic-Form Games

Strategic-Form

A game in *strategic-form* is an ordered triple, $G = (N, (S_i)_{i \in N}, (u_i)_{i \in N})$ in which:

- N=$\{$1,2,...,n$\}$ is a finite set of players.
- S_i is the set of strategies of player i, for every $i \in N$.
  Denote the set of all vectors of strategies by $S = S_1 \times S_2 \times ... \times S_n$.
- $u_i : S \to \mathbb{R}$ is a utility function.

Strategic-Form Games

Strategic-Form

A game in *strategic-form* is an ordered triple, $G = (N, (S_i)_{i \in N}, (u_i)_{i \in N})$ in which:

- N={1,2,...,n} is a finite set of players.
- S_i is the set of strategies of player i, for every $i \in N$.
  Denote the set of all vectors of strategies by $S = S_1 \times S_2 \times ... \times S_n$.
- $u_i : S \rightarrow \mathbb{R}$ is a utility function.

		Player II	
		A_{II}	B_{II}
Player I	A_I	0,1	1,0
	B_I	1,2	2,3

Figure: Simple Game in Strategic-Form

Nash Equilibrium

Nash Equilibrium

A strategy vector $s^* = (s_1^* \dots s_n^*)$ is a *Nash Equilibrium* if for each player $i \in N$ and each strategy $s_i \in S_i$, $u_i(s^*) \geq u_i(s_i, S_i^*)$ is satisfied.

		Player II	
		A_{II}	B_{II}
Player I	A_{I}	0,1	1,0
	B_{I}	1,2	2,3

Figure: Simple Game in Strategic-Form

Nash Equilibrium

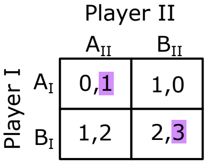
- If Player I plays strategy A_I, player II's best reply is A_{II}.

		Player II	
		A_{II}	B_{II}
Player I	A_I	0,1	1,0
	B_I	1,2	2,3

Figure: Simple Game in Strategic-Form

Nash Equilibrium

- If Player I plays strategy B_I, player II's best reply is B_{II}.



		Player II	
		$\mathrm{A_{II}}$	$\mathrm{B_{II}}$
Player I	$\mathrm{A_I}$	0,1	1,0
	$\mathrm{B_I}$	1,2	2,3

Figure: Simple Game in Strategic-Form

Nash Equilibrium

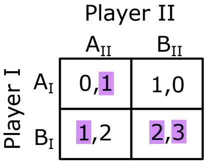
- If Player II plays strategy A_{II}, player I's best reply is B_I.

		Player II	
		$\mathrm{A_{II}}$	$\mathrm{B_{II}}$
Player I	$\mathrm{A_I}$	0,1	1,0
	$\mathrm{B_I}$	1,2	2,3

Figure: Simple Game in Strategic-Form

Nash Equilibrium

- If Player II plays strategy B_{II}, player I's best reply is B_I.



		Player II	
		A_{II}	B_{II}
Player I	A_I	0,1	1,0
	B_I	1,2	2,3

Figure: Simple Game in Strategic-Form

Hypergames

Hypergames

A simple hypergame H is given by $(N, (G^i)_{i \in N})$, where:

- $N = \{1, \ldots, n\}$ is a set of agents involved in the situation,
- $G^i = (N^i, S^i, u^i)$ is the subjective game of agent i, where:
  - N^i is a set of agents perceived by agent i.
  - $S^i = \times_{j \in N^i} S^i_j$ is a set of strategies perceived by agent i, where S^i_j is a set of strategies of agent j perceived by agent i.
  - $u^i = (u^i_j)_{j \in N^i}$ is a profile of utility functions perceived by agent i, where $u^i_j : S^i \to \mathbf{R}$ is agent j's utility function perceived by agent i.

Hypergames

German Strategies	Allied Strategies	
	RML	MN
AML	1,4	2,3
AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

German Strategies	Allied Strategies		
	RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

Hypergames

		Allied Strategies	
		RML	MN
German Strategies	AML	1,4	2,3
	AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

		Allied Strategies		
		RML	MN	N+C
German Strategies	AML	1,4	2,3	2,3
	AN	4,1	3,2	3,2
	AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

$$H = (N, (G^i)_{i \in N}), \; N = \{1, 2\}$$

Hypergames

Allied Strategies

German Strategies	RML	MN
AML	1,4	2,3
AN	4,1	3,2

Allies’ game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

Allied Strategies

German Strategies	RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies’ game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

$$H = (N, (G^i)_{i \in N}), \; N = \{1, 2\}$$
$$G^1 = (N^1, S^1, u^1) \text{ where } N^1 = \{2\}, S^1 = S^1_2 = \{RML, MN, N + C\}$$

Hypergames

	Allied Strategies	
German Strategies	RML	MN
AML	1,4	2,3
AN	4,1	3,2

	Allied Strategies		
German Strategies	RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

$$H = (N, (G^i)_{i \in N}), \;\; N = \{1, 2\}$$
$$G^1 = (N^1, S^1, u^1) \text{ where } N^1 = \{2\}, S^1 = S^1_2 = \{RML, MN, N + C\}$$
$$G^2 = (N^2, S^2, u^2) \text{ where } N^2 = \{1\}, S^2 = S^2_1 = \{AML, AN\}$$

Hyper-Nash Equilibrium

Hyper-Nash Equilibrium

There exists a hyper Nash equilibrium, $(s_i^{i*})_{i\in N} \in \times_{j\in N} S_j^j$, of a hypergame H iff $\forall i \in N,\ s_i^{i*} \in \mathbf{N}(G^i)_i$.

Set of Hyper-Nash Equilibrium

$\mathbf{HN}(H) = \times_{i\in N}\mathbf{N}(G^i)_i$ of hypergame H.

Hyper-Nash Equilibrium

Allied Strategies

German Strategies	RML	MN
AML	1,4	2,3
AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

Allied Strategies

German Strategies	RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

$$\mathbf{N}(G^1)_1 = \{AN, N + C\},\ \mathbf{N}(G^2)_2 = \{AN, MN\},$$

Hyper-Nash Equilibrium

German Strategies \ Allied Strategies	RML	MN
AML	1,4	2,3
AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

German Strategies \ Allied Strategies	RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

$$\mathbf{N}(G^1)_1 = \{AN, N+C\},\ \mathbf{N}(G^2)_2 = \{AN, MN\},$$
$$\mathbf{HN}(H) = \mathbf{N}(G^1)_1 \times \mathbf{N}(G^2)_2 = \{AN, MN\}$$

Stable Hyper-Nash Equilibrium

Stable Hyper-Nash Equilibrium

There exists a stable hyper Nash equilibrium, $(s_i^{i**})_{i \in N} \in \times_{j \in N} S_j^j$, of a hypergame H iff
$\forall k \in N, (s_i^{i**})_{i \in N} \in \mathbf{N}(G^k)$.

Set of Stable Hyper-Nash Equilibrium

$\mathbf{SHN}(H) = \cap_{i \in N} \mathbf{N}(G^i)$.

Stable Hyper-Nash Equilibrium

German Strategies	Allied Strategies: RML	MN
AML	1,4	2,3
AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

German Strategies	Allied Strategies: RML	MN	N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

No stable Nash equilibria exists in this game as $\mathbf{SHN}(H) = \mathbf{N}(G^1) \cap \mathbf{N}(G^2) = \emptyset$.

Stable Hyper-Nash Equilibrium

German Strategies	Allied Strategies: RML	Allied Strategies: MN
AML	1,4	2,3
AN	4,1	3,2

Allies' game:
AML =Attack Maginot Line
AN =Attack in North
RML = Reinforce Maginot Line
MN = Move North

German Strategies	Allied Strategies: RML	Allied Strategies: MN	Allied Strategies: N+C
AML	1,4	2,3	2,3
AN	4,1	3,2	3,2
AA	3,2	5,0	2,3

German game:
AML, AN, RML, MN = As in Allies' game
AA = Attack through Ardennes
N + C = Go North, but then counterattack behind Ardennes

Figure: A simple two-player hypergame

No stable Nash equilibria exists in this game as $\mathbf{SHN}(H) = \mathbf{N}(G^1) \cap \mathbf{N}(G^2) = \emptyset$.
This means that the hypergame H is an unstable hypergame.

A Simple Cybersecurity example

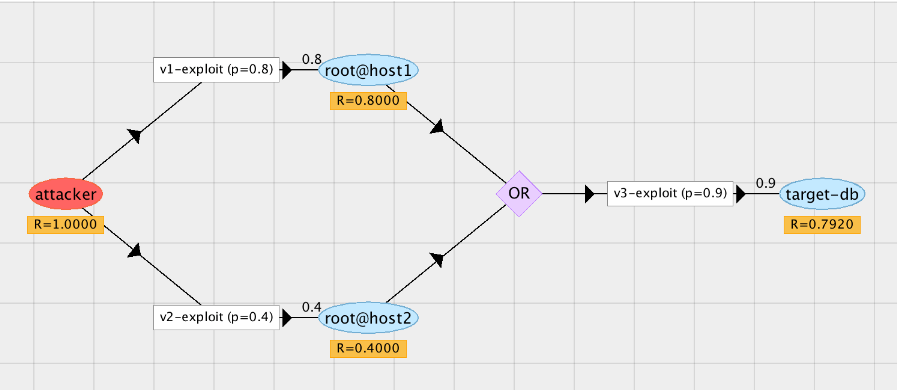


Figure: The Cyber attack graph from the Defenders Perspective

A Simple Cybersecurity example

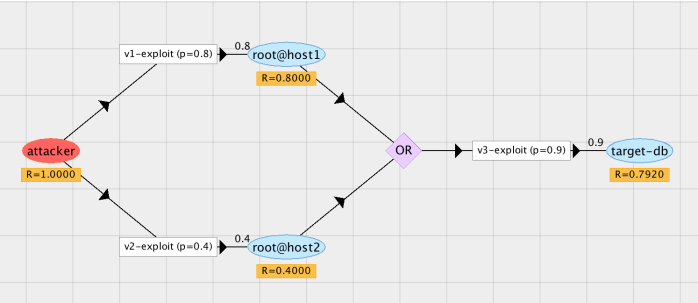


Figure: The Cyber attack graph from the Defenders Perspective

Attackers: V1V3, V2V3
Defenders: Host1, Host2, Target

A Simple Cybersecurity example

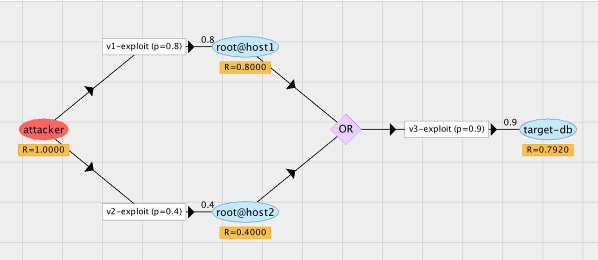


Figure: The Cyber attack graph from the Defenders Perspective

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13

A Simple Cybersecurity example

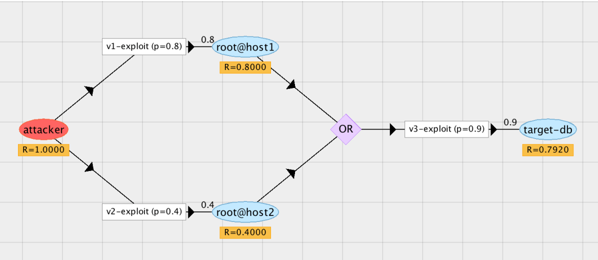


Figure: The Cyber attack graph from the Defenders Perspective

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9

A Simple Cybersecurity example

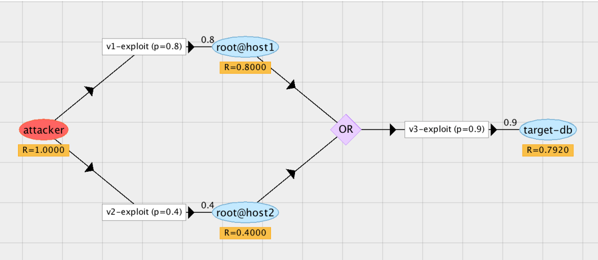


Figure: The Cyber attack graph from the Defenders Perspective

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9
Defenders Expected Values; Host1: 6, Host2: 7, Target: 10

A Simple Cybersecurity example

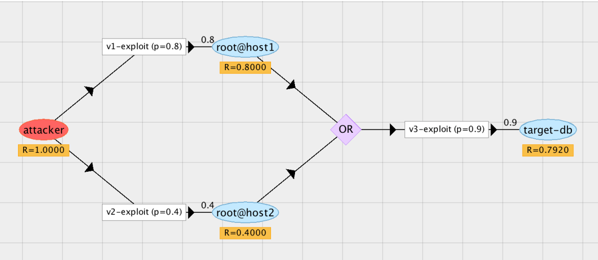


Figure: The Cyber attack graph from the Defenders Perspective

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9
Defenders Expected Values; Host1: 6, Host2: 7, Target: 10
Defenders Costs; Host1: 5, Host2: 6, Target: 9

A Simple Cybersecurity example

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9
Defenders Expected Values; Host1: 6, Host2: 7, Target: 10
Defenders Costs; Host1: 5, Host2: 6, Target: 9

V1V3 and Host1; Defender: $6 + 7 + 10 - 5 = 18$, Attacker: -4

Attacker

Defender	V1V3	V2V3
Host1	18,-4	1,4
Host2	1,4.4	17,-6
Target	8,-4.6	7,-5

Figure: The Hypergame from the Defenders Perspective

A Simple Cybersecurity example

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9
Defenders Expected Values; Host1: 6, Host2: 7, Target: 10
Defenders Costs; Host1: 5, Host2: 6, Target: 9

V1V3 and Host2; Defender: $7 - 6 = 1$, Attacker: $11.4 - 7 = 4.4$

		Attacker	
		V1V3	V2V3
Defender	Host1	18,-4	1,4
	Host2	1,4.4	17,-6
	Target	8,-4.6	7,-5

Figure: The Hypergame from the Defenders Perspective

A Simple Cybersecurity example

Attackers Expected Values; V1: $3 \times 0.8 = 2.4$, V2: $10 \times 0.4 = 4$, V3: $10 \times 0.9 = 9$. Overall: V1V3: 11.4, V2V3:13
Attackers Costs; V1: 4, V2: 6, V3:3. Overall: V1V3: 7, V2V3:9
Defenders Expected Values; Host1: 6, Host2: 7, Target: 10
Defenders Costs; Host1: 5, Host2: 6, Target: 9

V1V3 and Target; Defender; $7 + 10 - 9 = 8$, Attacker: $2.4 - 7 = -4.6$

		Attacker	
		V1V3	V2V3
Defender	Host1	18,-4	1,4
	Host2	1,4.4	17,-6
	Target	8,-4.6	7,-5

Figure: The Hypergame from the Defenders Perspective

A Simple Cybersecurity example

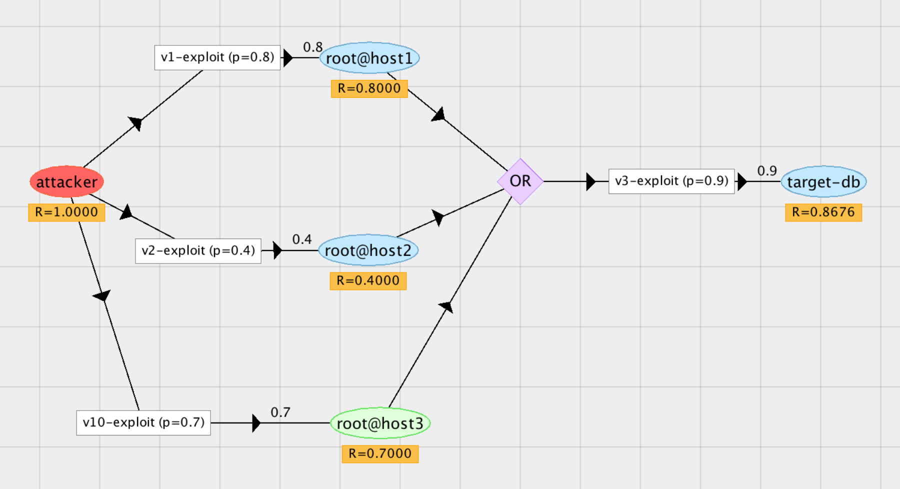


Figure: The Cyber attack graph from the Attackers Persective

A Simple Cybersecurity example

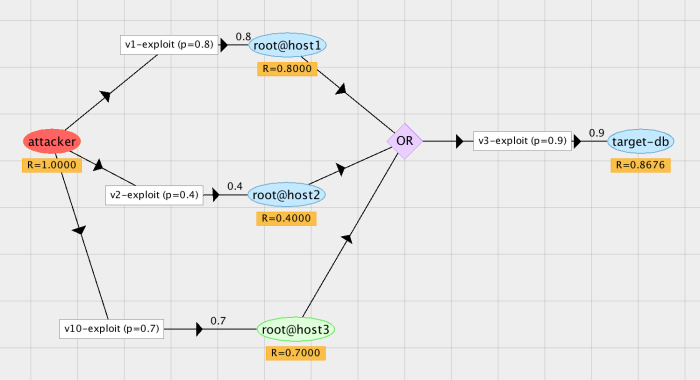


Figure: The Cyber attack graph from the Attackers Persective

Attackers: V1V3, V2V3, V10V3

Defenders: Host1, Host2, Host3, Target

A Simple Cybersecurity example

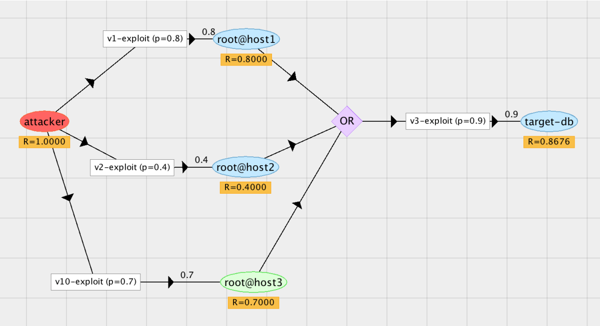


Figure: The Cyber attack graph from the Attackers Persective

Attackers Expected Values; V1: 2.4, V2: 4, V10: $5 \times 0.7 = 3.5$, V3: 9. Overall: V1V3: 11.4, V2V3:13, V10V3: 8

Attackers Costs; V1: 4, V2: 6, V10: 5, V3:3. Overall: V1V3: 7, V2V3:9, V10V3: 8

A Simple Cybersecurity example

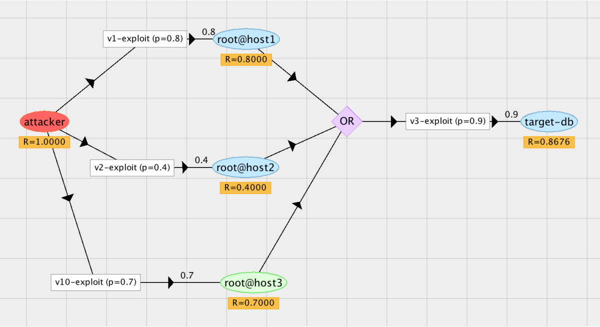


Figure: The Cyber attack graph from the Attackers Persective

Attackers Expected Values; V1: 2.4, V2: 4, V10: $5 \times 0.7 = 3.5$, V3: 9.
Overall: V1V3: 11.4, V2V3:13, V10V3: 8

Attackers Costs; V1: 4, V2: 6, V10: 5, V3:3. Overall: V1V3: 7, V2V3:9, V10V3: 8

Defenders Expected Values; Host1: 6, Host2: 7, Host3:9, Target: 10

Defenders Costs; Host1: 5, Host2: 6, Host3:7, Target: 9

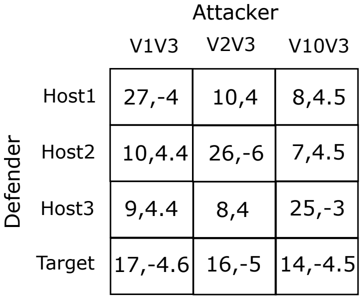
A Simple Cybersecurity example

Attackers Expected Values; V1: 2.4, V2: 4, V10: $5 \times 0.7 = 3.5$, V3: 9. Overall: V1V3: 11.4, V2V3:13, V10V3: 8

Attackers Costs; V1: 4, V2: 6, V10: 5, V3:3. Overall: V1V3: 7, V2V3:9, V10V3: 8

Defenders Expected Values; Host1: 6, Host2: 7, Host3:9, Target: 10

Defenders Costs; Host1: 5, Host2: 6, Host3:7, Target: 9



	Attacker		
Defender	V1V3	V2V3	V10V3
Host1	27,-4	10,4	8,4.5
Host2	10,4.4	26,-6	7,4.5
Host3	9,4.4	8,4	25,-3
Target	17,-4.6	16,-5	14,-4.5

Figure: The Hypergame from the Attackers Perspective

A Simple Cybersecurity example

		Attacker	
		V1V3	V2V3
Defender	Host1	18,-4	1,4
	Host2	1,4.4	17,-6
	Target	8,-4.6	7,-5

		Attacker		
		V1V3	V2V3	V10V3
Defender	Host1	27,-4	10,4	8,4.5
	Host2	10,4.4	26,-6	7,4.5
	Host3	9,4.4	8,4	25,-3
	Target	17,-4.6	16,-5	14,-4.5

Figure: The Hypergame

Thank You
Any Questions?