• Bruce Large

SESSION 18B

ON THE ART OF GAME THEORY & THREAT MODELLING

/WHOAMI

- Director and Principal Cyber Security Architect at BLARGE
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for over 15 years
- I have a strong interest in Cyber Security Architecture, Cyber Threat Intelligence and Active Defense
- Proud member of Professionals Australia – join your #STEMUNION
- Experience in Electricity Generation & Transmission, Railway, Aviation, Emergency Services and Consulting industries

AGENDA

1. An overview of Game Theory
2. A Primer on Threat Modelling
3. How to use Game Theory with Threat Modelling

WHY THIS PRESENTATION?

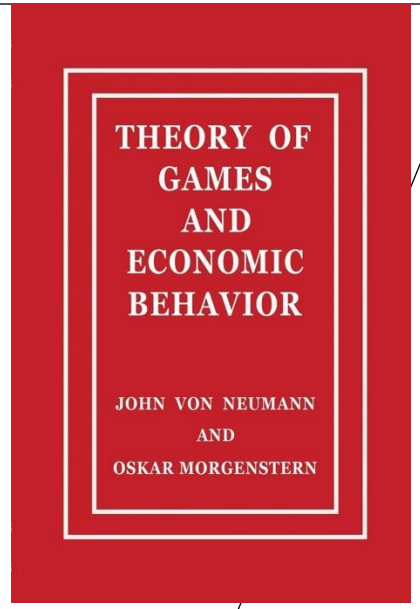
AN OVERVIEW OF GAME THEORY

A SHORT HISTORY OF GAME THEORY

The 1944 “Theory of Games and Economic Behaviour” by Von Neumann and Morgenstern is an ground breaking publication

It used Mathematical Models to analyse strategies and behaviour of players – but there are some challenges to the theory like assuming rational behaviour of players and their access to perfect information

Has been extended in Modern Game Theory in in the 1950s by the RAND corporation



SO, WHAT MAKES A GAME?

Elements of a Game:

- **Players –** Who is involved in the "game"
- **Strategies –** What possible actions do the players have
- **Payoffs –** Rewards and outcomes
- **Information –** What do players know

Types of Games:

- **Zero Sum Games –** One Player Wins, the other Loses - These are often the most relevant for Cyber Security Use Cases
- **Non-Zero Sum Games –** Outcomes can be mutually beneficial or harmful
- **Cooperative Games –** You can form an alliance and gang up (This is a great cyber defence Game)
- **Non-Cooperative Games –** All players work alone and independent

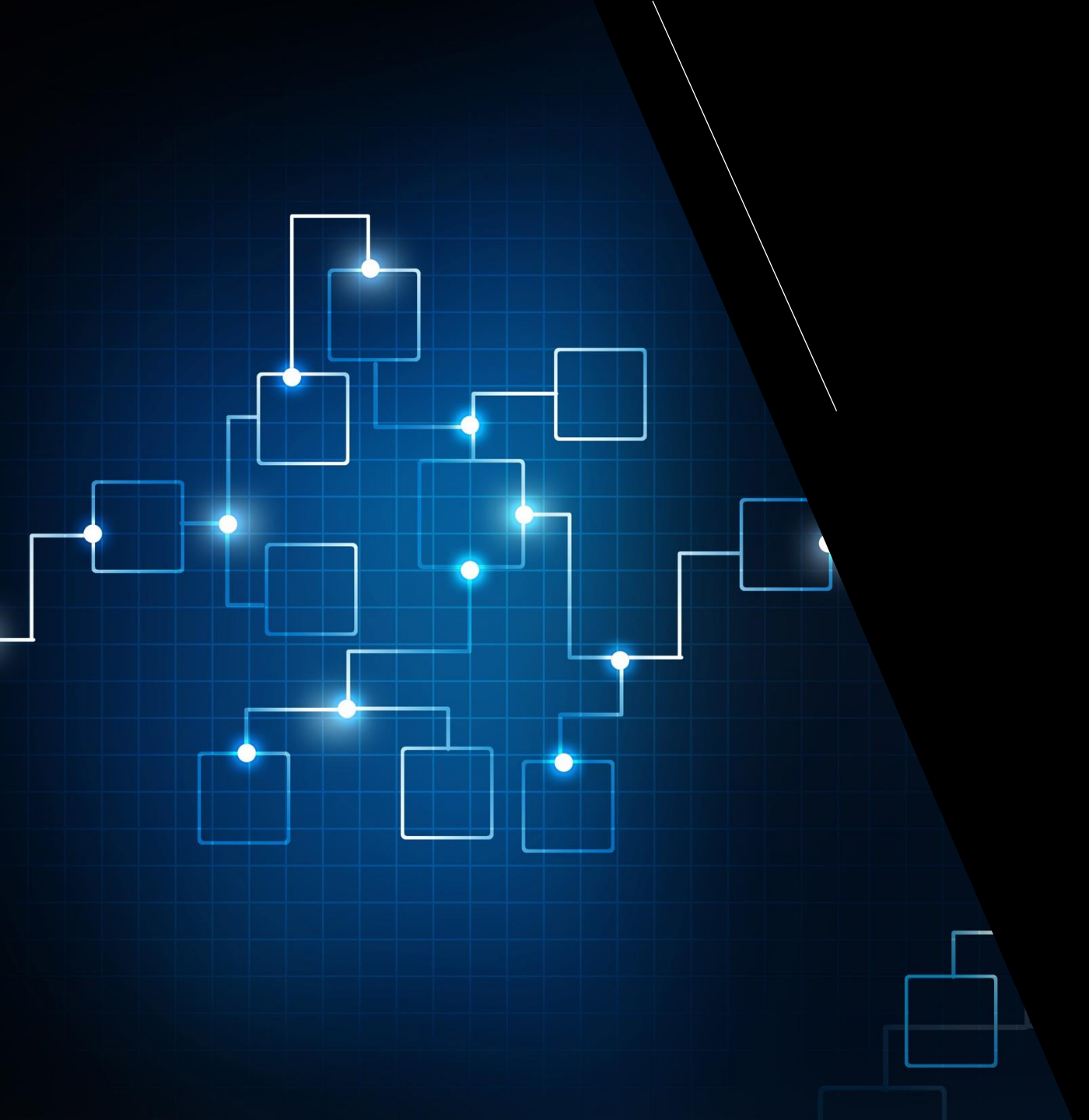
APPLICATION TO MILITARY DEFENSE AND NUCLEAR DETERRENCE

- Game theory was used to analyse the strategy for Nuclear Deterrence to figure out the best strategies to avoid Mutually Assured Destruction
- It did this by understanding the players, their strategies and payoffs for this Zero-Sum Game (even though eventually we both lose)

THE PRISONER DILEMMA

- **Two people are detained, they can not talk to each other, the game is:**
  - If both people confess they get 5 years
  - If the person says the other person did it they get 0 years and the other person gets 8 years
  - If both people say nothing, they are both assumed somewhat guilty and get 1 year

		Person 1	
		Confess	Don’t Confess
Person 2	Confess	[5,5]	[0,8]
	Don’t Confess	[0,8]	[1,1]



A PRIMER ON THREAT MODELLING

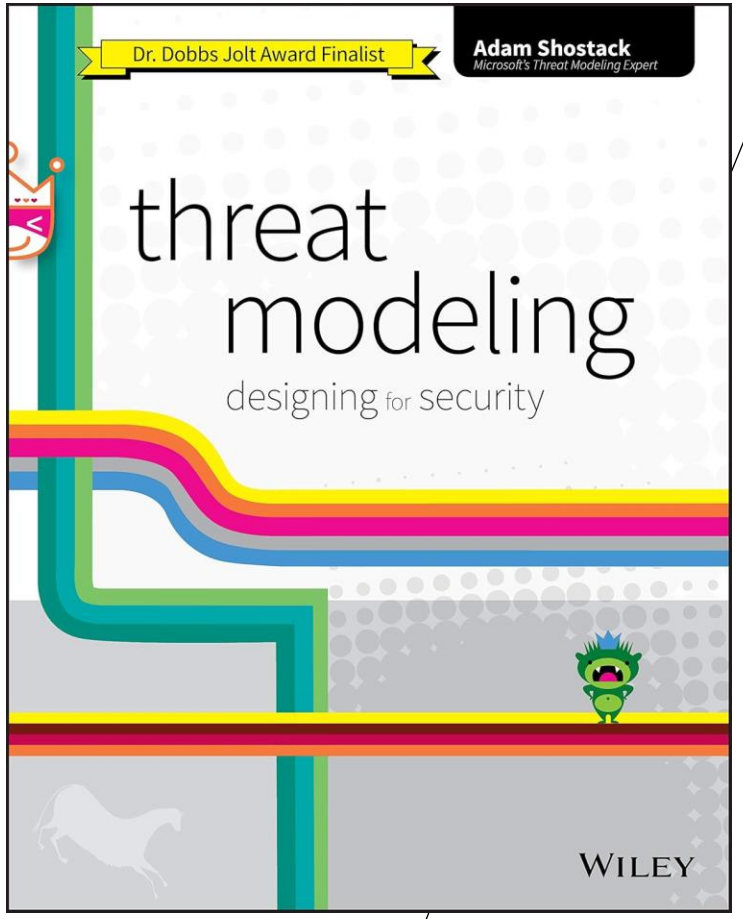
WHAT IS A THREAT?

Ref – SANS ICS515

SHOSTACKS THREAT MODELLING REFERENCE

Three Types of Threat Modelling

- **Asset Based**
  - Things Attackers Want
  - Things you want to protect
  - Stepping Stones
- **Attacker Based**
  - Consider Attacker Personas
- **Software Focused**
  - Use tools like STRIDE



Ref - https://www.amazon.com.au/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998

EXAMPLE DATA FLOW DIAGRAM MODEL & STRIDE

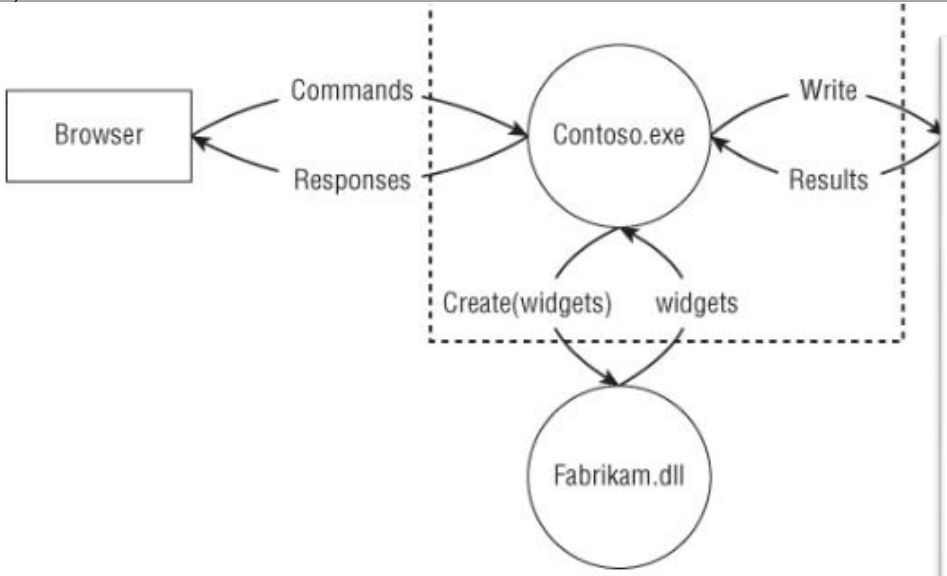


Figure 3-1: The system referenced in Table 3-10

Table 3-11: STRIDE-per-Interaction (Example)

	ELEMENT	INTERACTION	S	T	R
1	Process (Contoso)	Process has outbound data flow to data store.	"Database" is spoofed, and Contoso writes to the wrong place.		
2		Process sends output to other process.	Fabrikam is spoofed, and Contoso writes to the wrong place.		Fabrikam claims not have been called by Contoso.
3		Process sends output to	Contoso is confused		Browser disclaims a

Ref – Shostack Threat Modelling

EXAMPLE ATTACK TREES

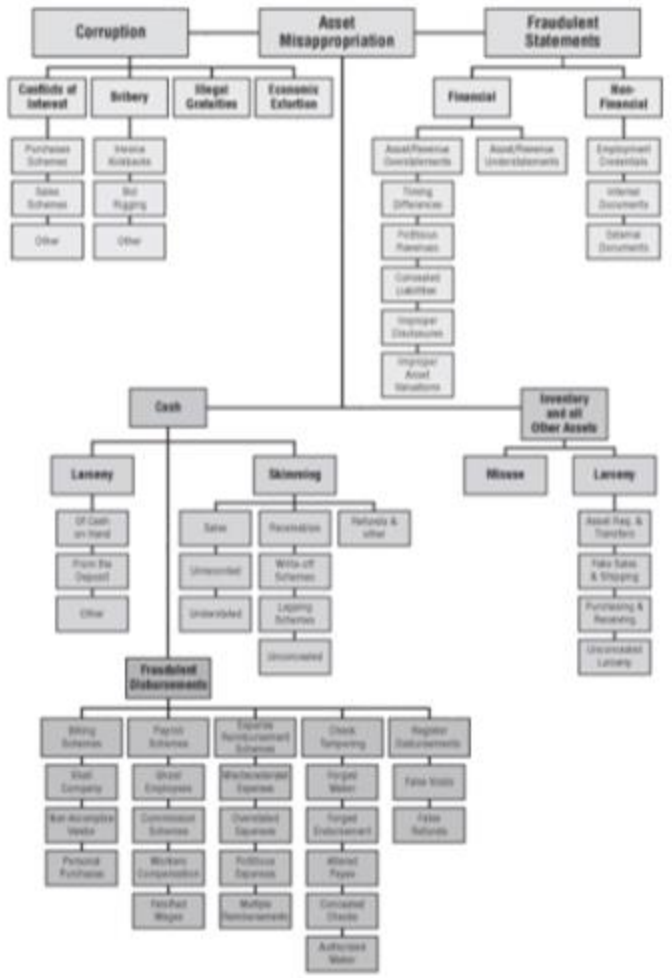


Figure 4.2 A tree drawn on a grid

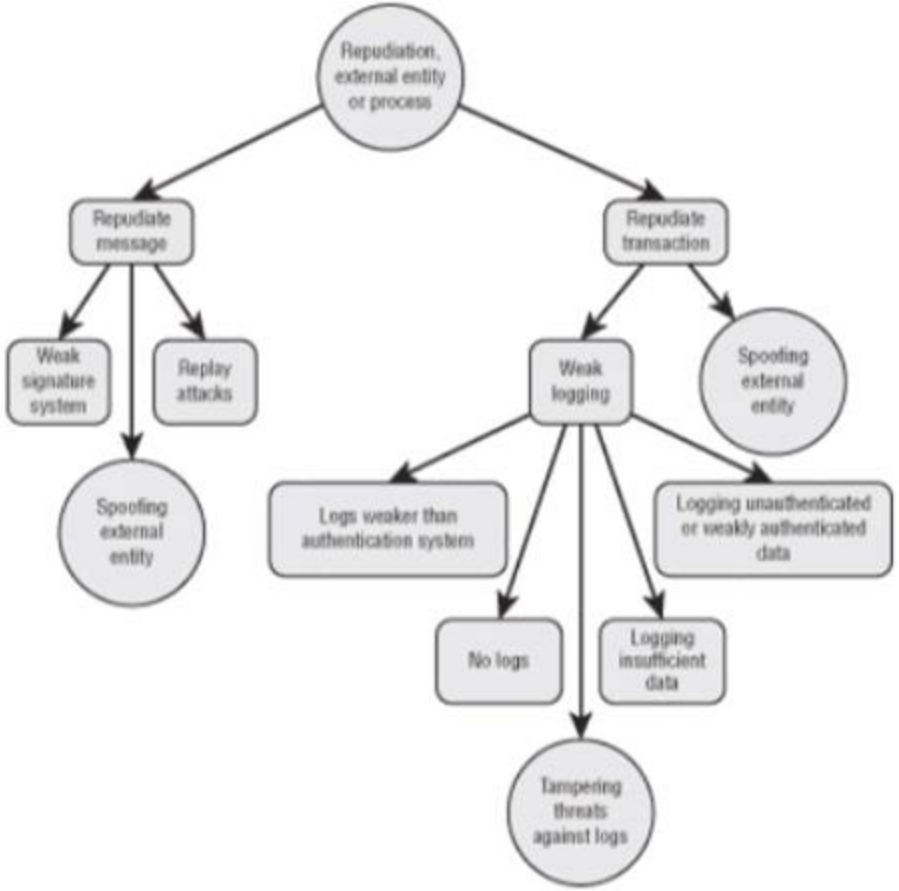


Figure 4-3: A tree drawn without a grid

Ref – Shostack Threat Modelling

ATTACK PATHS WITH CCE

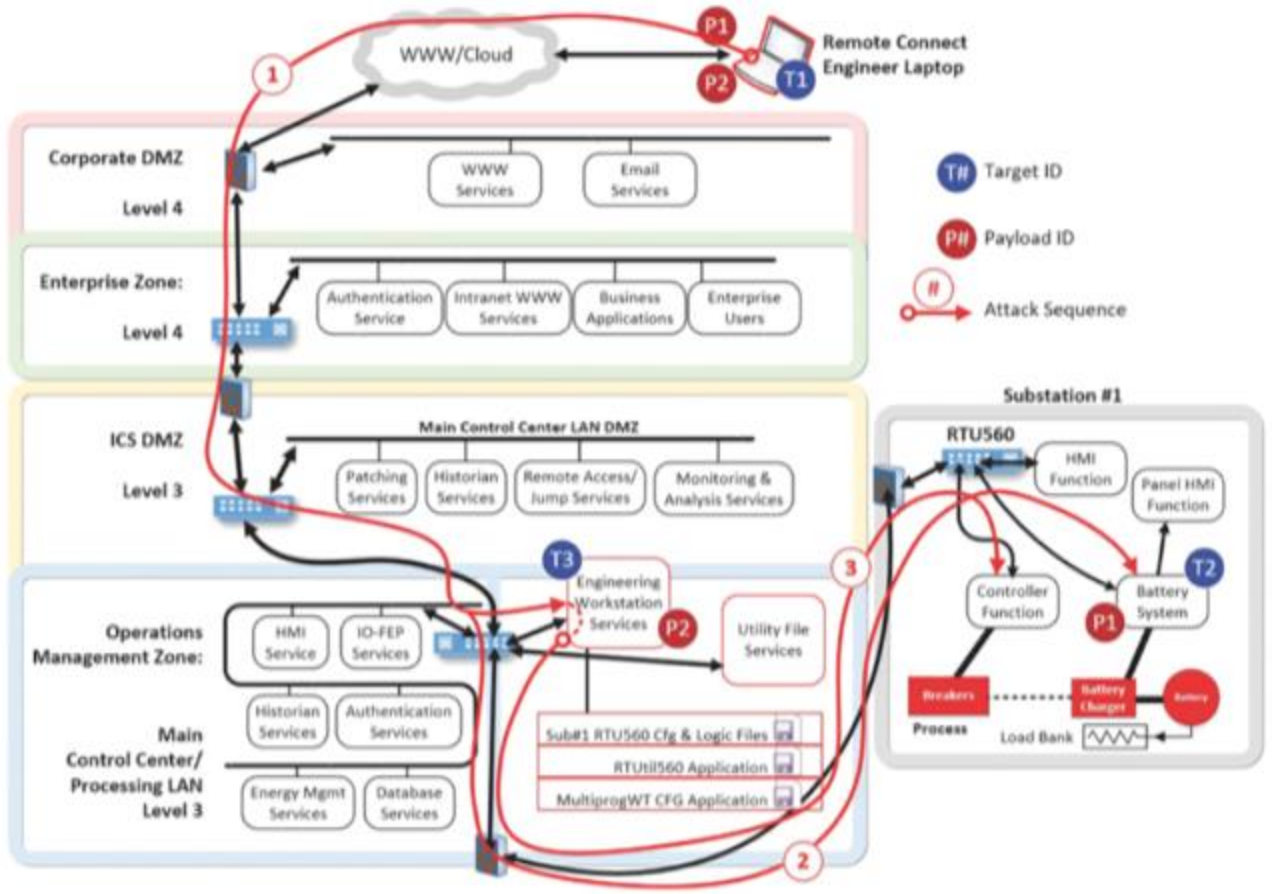


Figure A.16 HCE Attack Communications Path via SCADA to Sub#1 Battery System and RTU560 Station.

Ref - Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)

HOW TO USE GAME THEORY WITH THREAT MODELLING

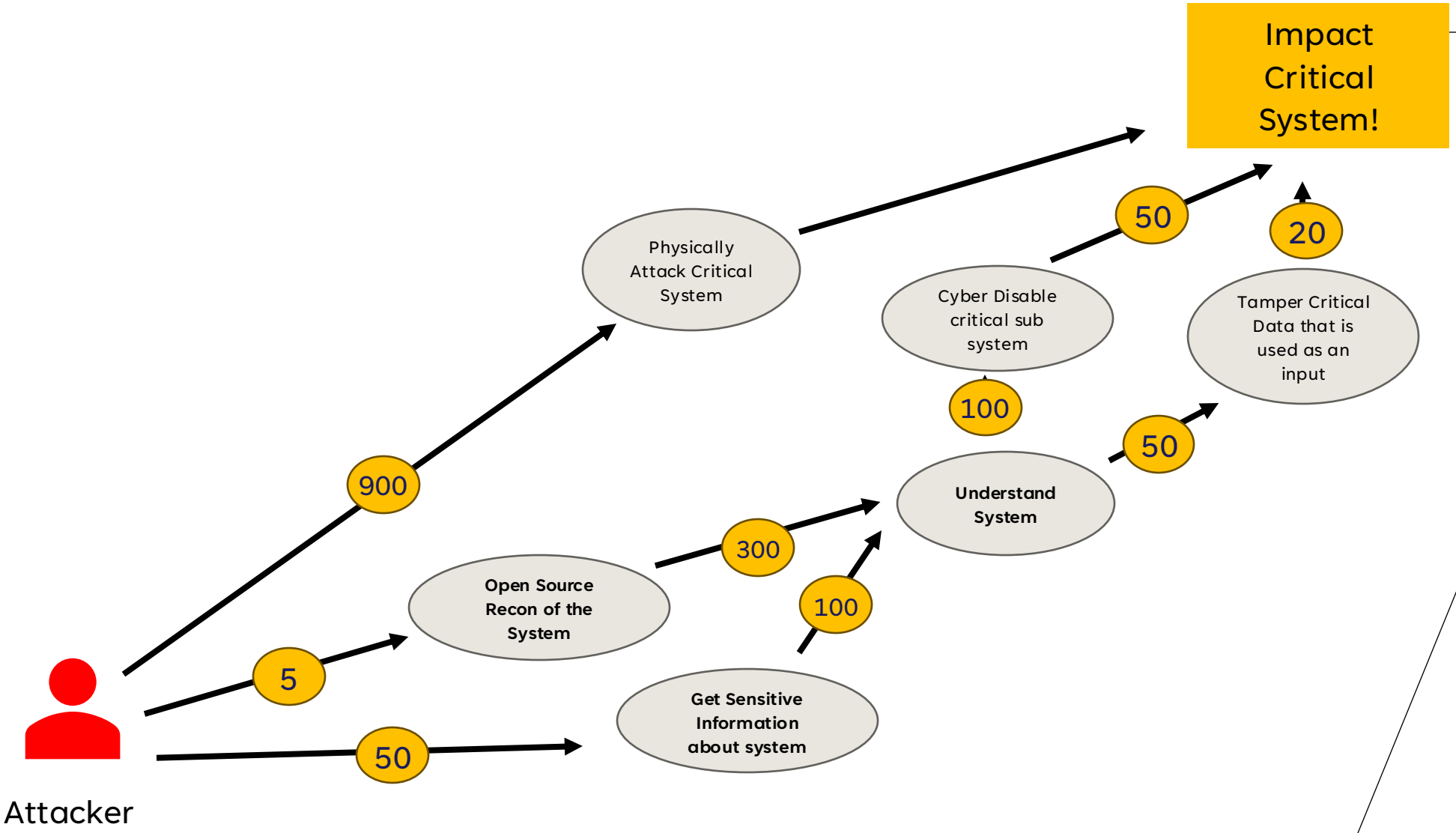
OUR SCENARIO FOR TODAY

- Let’s consider we are a Critical Infrastructure Provider
- We have a critical business function that will disrupt the national economy if it is compromised
- The system is not well known to the general public, but, is used globally and follows a known architecture

THREAT MODELLING WITH GAME THEORY

- Who are the Players?
- What are the Payoffs?
- What is the style of the game?
- How can I increase the cost for the attacker?
- How can I decrease their payoff?

GAME THEORY THREAT MODEL



GROUP DISCUSSION

THANK YOU

Bruce Large

https://linkedin.com/in/blargeau

bruce@blarge.io

https://github.com/beLarge

https://blarge.io

SESSION FEEDBACK

- Paper feedback forms are available from the front of the room

OR
cosac.bz/feedback