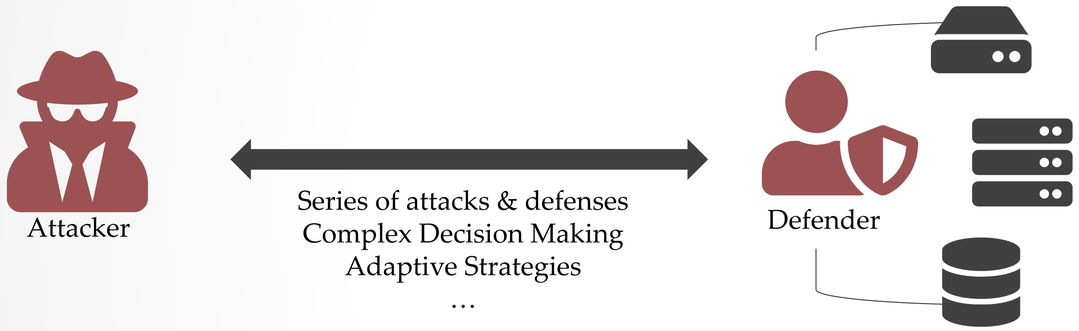
Game Theory Applications within Cyber Security

Erhan Tezcan 0070881 – Mandana Bagheri Marzijarani 0074025

Problem: Complex Decision-Making Strategies of Attacker & Defender

The number of incidents in cyberspace is constantly rising. Most defense methods in practice are ad hoc, which are often destined to be circumvented by more clever and novel attacks.



The Attacker (a group of entities such as botnet / a human / a malware / …) tries to **engage in malicious activity**.
The Defender (IDS / anti-virus / system administrator / security expert / …) tries to **prevent** that from happening.

More advanced attacks result in a series of actions, based on *complex decision making* and *dynamic interactions*. Static defense mechanisms against known attacks are always **vulnerable** to such dynamic and novel attacks.

Game theory deals with optimal decision making of independent players. Complex attack-and-defend schemes can be modeled and studied under game theory.

Solution: Security Setting modeled as a Game and studied under Game Theory

1. Model the attack setting as a **game** (or many games)
2. Formally define the **players** and **payoffs**
3. Prove and try to find the **equilibrium points**
4. Create **strategies**

Payoffs

	D	**¬D**
A	0,-2	-5,5
¬A	-3,0	1,0

A: Attack ¬ A: No Attack
D: Defense ¬ D: No Defense

Classificiation		Information	Application
Cooperative	Static	Imperfect	[6]
Non-Cooperative	Static	Complete Imperfect	[7], [8]
		Incomplete Imperfect	[9], [10]
	Dynamic	Complete Perfect	[11]–[14]
		Complete Imperfect	[15]
		Incomplete Perfect	[16]–[19]
		Incomplete Imperfect	[20]–[23]

We provide classification of games and survey its applications.
We focus on 3 particular studies:

1. An intrusion detection network resource allocation model
2. A detection manipulation game
3. A moving target defense for intrusion detection system placement on cloud systems

We make remarks on similarities between *cryptographical assumptions* & *reduction proofs* and *formal definitions of game models* & *existence of equilibrium points* in them.