How Shall We Play a Game?

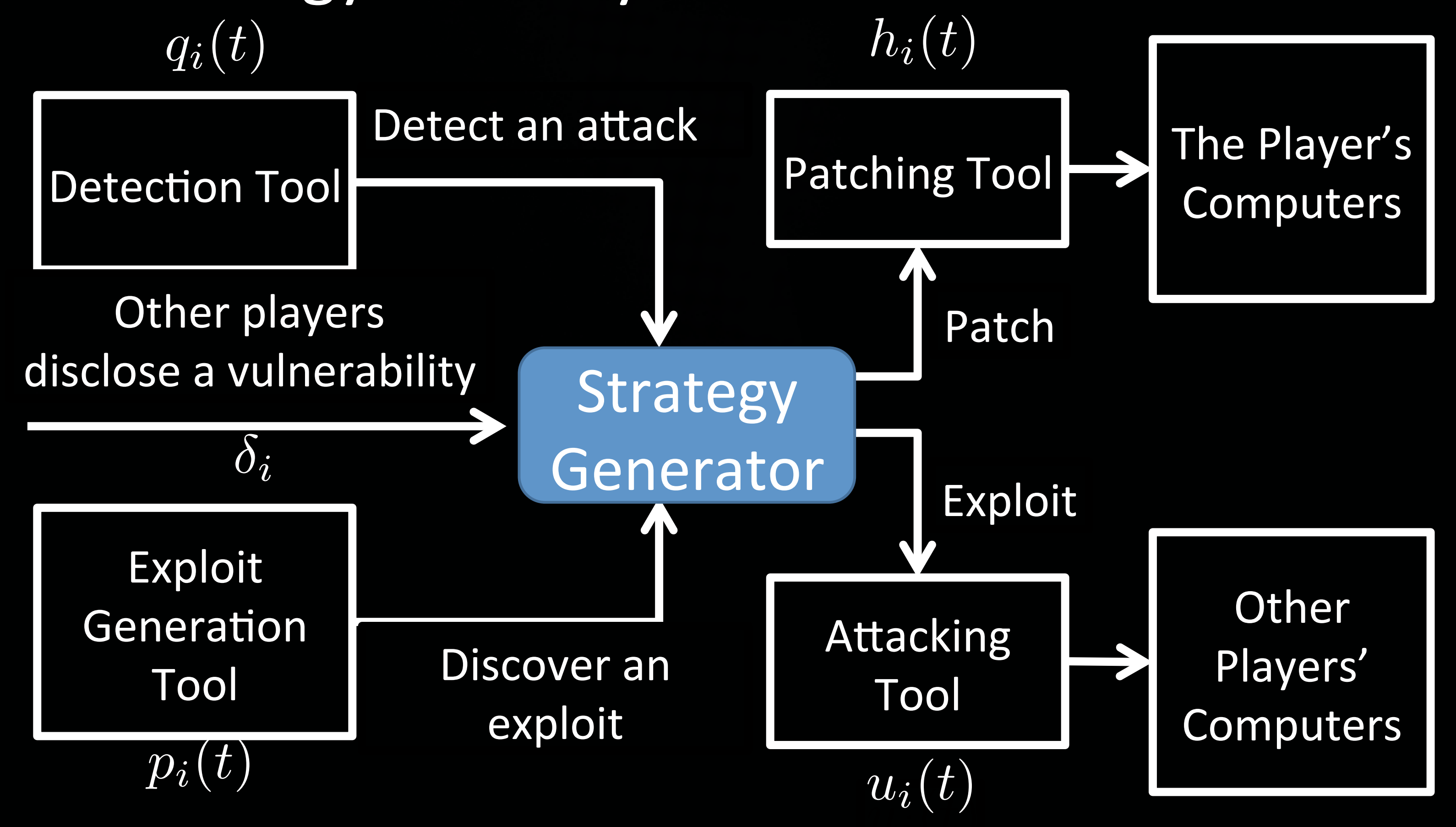
A Game-theoretical Model for Cyber-warfare Games

Tiffany Bao[1], Yan Shoshitaishvili[2], Ruoyu Wang[2], David Brumley[1]

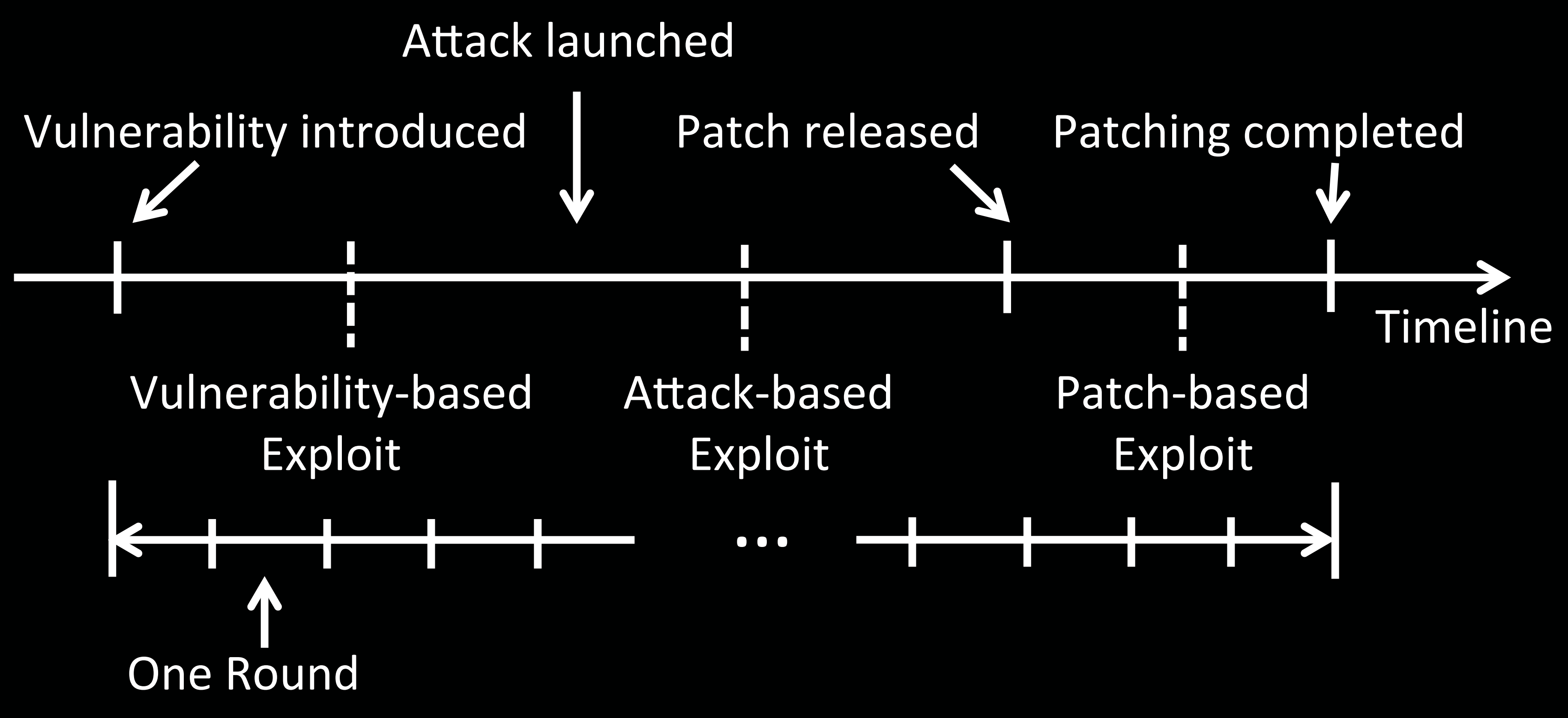
[1]Carnegie Mellon University, [2]University of California, Santa Barbara

Goals

- Fully Autonomous Systems becomes possible: Mayhem in the Cyber Grand Challenge.
- The Strategy Generator is a key component to instruct the system.
- The goal is to **automatically** find the best strategy of the system.



The Cyber-warfare Game in Multiple Rounds



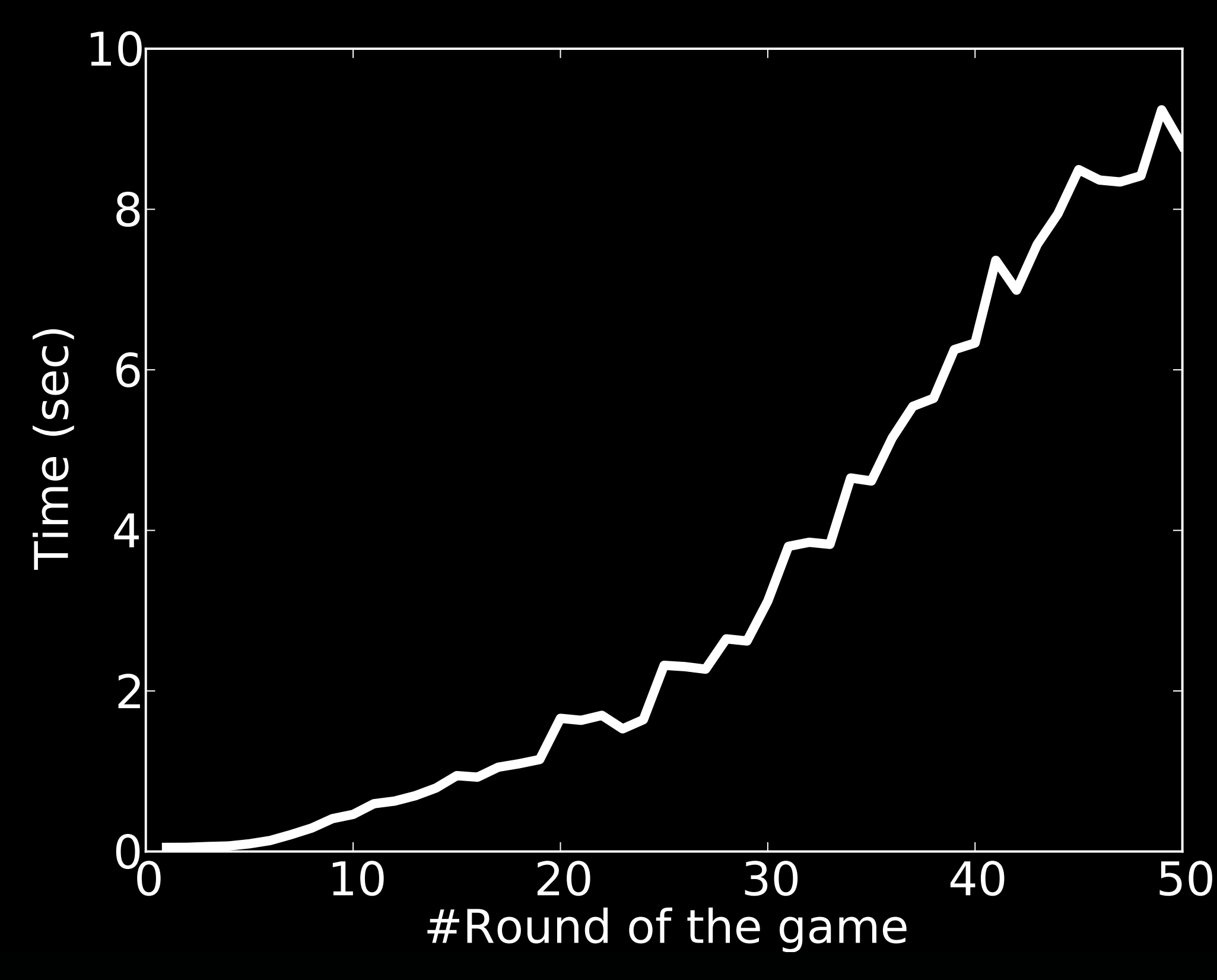
- Partial Observable Stochastic Game (POSG)
  - Players do not know if the other players have discovered a vulnerability or the other players' actions.
- Finding the best strategy of POSG: PPAD-hard problem (which cannot be scalable).
- We divide the game into two sub-games in order to find the best strategy by dynamic programing.
  - Sub-game 1: before vulnerability disclosure
  - Sub-game 2: after vulnerability disclosure

Game Parameters

Parameter	Definition
$p_i(t)$	The probability distribution over time that player i discovers a vulnerability at round t.
$q_i(t)$	The probability to launch a ricochet attack with exploits that player i received in the previous round.
$h_i(t)$	The ratio of the amount of patched vulnerable resources over the total amount of vulnerable resources at round t.
δ_i	The number of rounds required by player i to generate a patch-based exploit after a vulnerability and the corresponding patch are disclosed.
$u_i(t)$	The dynamic utility that player i gains by attacking his opponents at round t.

Evaluation

- Performance: for a game with 50 time slots, we found the best strategy in 10 seconds.



- Observation: When a player discloses a vulnerability, the other players should attack right after they generate the attack.

SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING

Computational Cybersecurity in Compromised Environments
2016 Fall Workshop | October 17-19 | Atlanta, Georgia