Adaptive Self-guarded Honeypot

PhD Student : Sereysethy Touch (sereysethy.touch@unamur.be)
Supervisor : Prof. Jean-Noël Colin
Affiliation : Faculty of Computer Science, UNamur

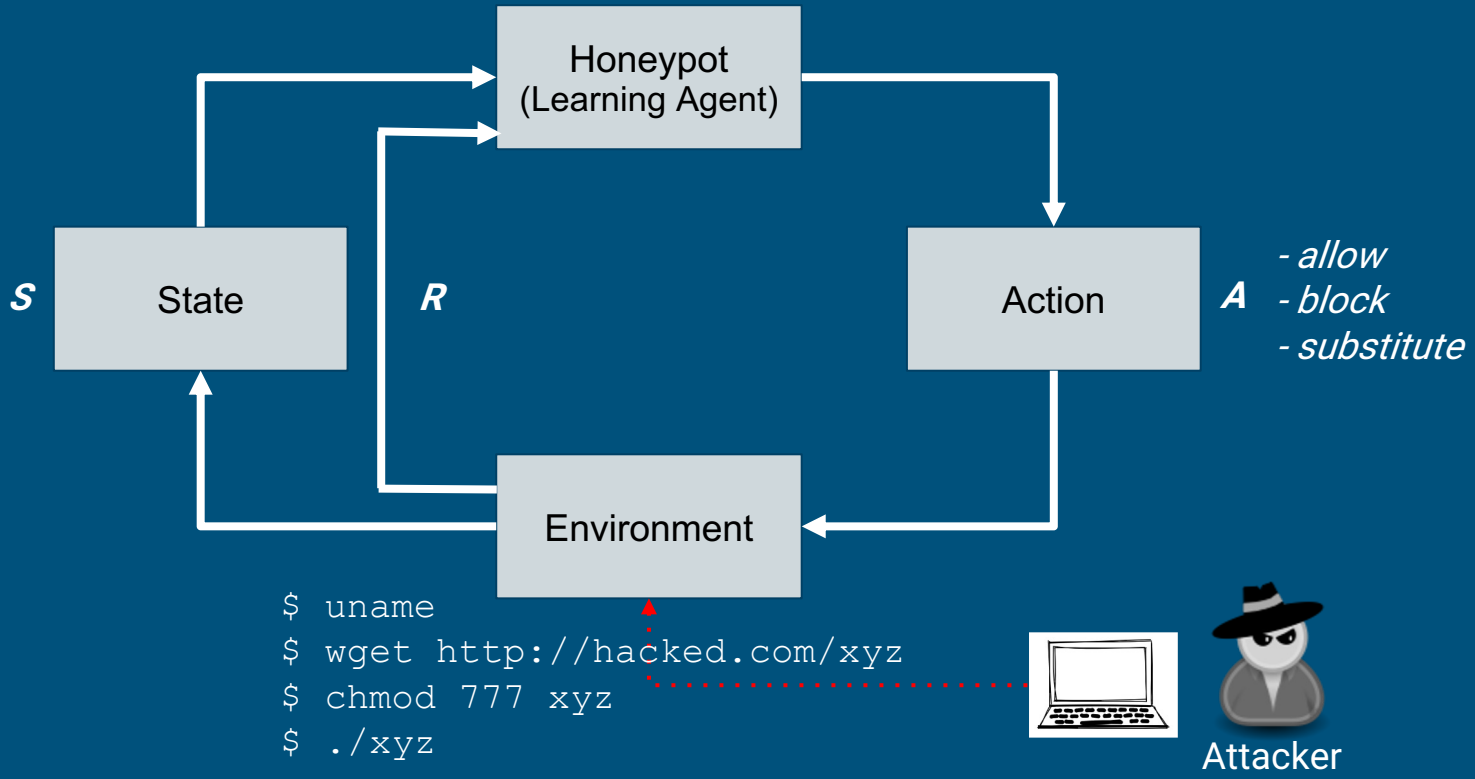
CyberExcellence, UMons, 08/11/2022

Research objective

Build an adaptive (smart) honeypot using the SSH protocol to achieve two primary objectives:

1. Interact with the attackers to collect their tools.
2. Defend itself from being deeply compromised.

Our approach: a honeypot as a RL agent



Our approach

- Different representations of the environment state
  - Only command
  - Command + arguments
  - Command + arguments + the honeypot environment (CPU, Memory, Network flows, etc.)
- Actions
  - Allow
  - Block
  - Substituer
  - Terminer
  - Nop
- Different reward functions
  - Simple: environment state and action
  - Complex: env. state, action, context, risk level, honeypot environments
- Learning algorithms
  - Model-Based
  - Model-Free
  - ...

First Result: Asgard (Touch & Colin, 2021)

- Simple environment state
  - command
- Action:
  - Allow
  - Block
  - Substitute
- Reward function
  - Environment state + action
- Learning Algorithm
  - Q-learning: a tabular function
- Evaluation (Touch & Colin, 2022)
  - Cowrie: a low-interaction honeypot
  - Real Linux System: a high-interaction honeypot
  - Midgard: a variant of Asgard

Challenges

- Rich environment state representation
  - How to effectively represent the command, its arguments and other honeypot parameters
- Complex reward function
  - How to combine different factors to reward the agent to learn
  - E.g: how to define a risk level associated to to each command
- Learning algorithm
  - When the state space and the action space increases, a more complex Q-function is also considered: a linear function and a neural network

Thank you

- Touch, S., & Colin, J. N. (2021, October). Asguard: Adaptive Self-guarded Honeypot. In *17th International Conference on Web Information Systems and Technologies-Volume 1: DMMLACS*, (pp. 565-574). SciTePress.
- Touch, S., & Colin, J. N. (2022). A Comparison of an Adaptive Self-Guarded Honeypot with Conventional Honeypots. *Applied Sciences, 12*(10), 5224