COMP2410/6340
Automated Decision Making & Cyber (Physical) Security – Part 3

Hanna Kurniawati

http://users.cecs.anu.edu.au/~hannakur/

Australian National University

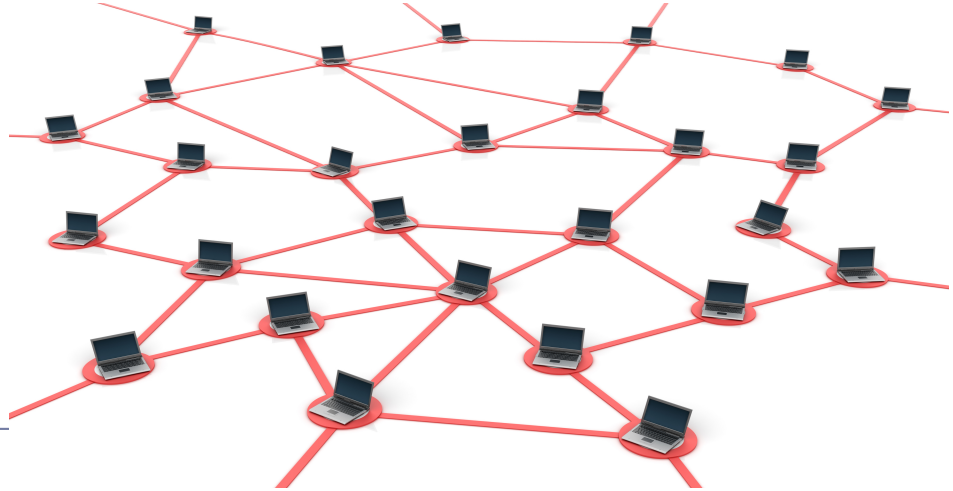
RESEARCH SCHOOL OF COMPUTER SCIENCE

This set of videos

- ✓ Part-1: Intro
  - ✓ Automated decision-making
- ✓ Part-2: Intro to POMDP
  - ✓ Framework for decision-making under uncertainty
  - ✓ Solving, aka. generating strategic decisions
- Part-3: Example of POMDP in Cyber security
  - Autonomous pen-testing

Penetration Testing (Pen-testing)

- Pen-testing (also known as ethical hacking) aims to identify vulnerabilities in a computer / computer network by emulating real attacks.
- A lucrative business / career ☺
  - The simplest ~A$5-6K, but it can go up fast [Source: https://www.gridware.com.au/penetration-testing/, https://www.securitymetrics.com/blog/how-much-does-pentest-cost]



Why autonomous?

- With computers and internet becoming ubiquitous, with high frequency updates and patches, pen-testing should be conducted often.
- However, many can’t afford to conduct pen-testing as often as they should
- Perhaps, if we can automate, we can conduct pen-testing (at least the simple ones) much more often
  - Not to replace human pen-testing, but to complement

Autonomous Pen-Testing

- The problem is essentially: How to assess and penetrate a computer / network, when the agent does not know the exact and full properties of the computer / network (e.g., what OS is running, what ports are open, etc.) nor the defender (e.g. the sysadmin) strategy for protecting the computer / network

Let’s take a simplified problem…

- Autonomous pen-testing of a computer where uncertainty comes from not knowing:
  - The exact and full properties of the environment (aka the computer): This causes non-deterministic transition and possible error in observation

Modeling the POMDP Agent

- Define the 6-tuples (S, A, O, T, Z, R):
  - State space (S): Computer properties. For instance,
    - $S = S_{ssh} \times S_{ftp} \times S_{OS} \times E$ where:
    - S_{ssh} and S_{ftp} are binary variables indicating whether ssh and ftp are installed or not, respectively
    - S_{os} is a variable indicating the operating system of the computer. The possible values can be one of {Win, Linux, Mac}
    - E is a binary variable indicating whether the computer has been successfully exploited
  - Action space (A): Possible command the pen-tester can use. For instance, {$scan_{ssh}$, $scan_{ftp}$, $scan_{os}$, breakPassword, accessComputer}
  - Observation space (O): The set of observation the agent can perceive, e.g., {ssh_port is open, ssh_port is closed, the operating system, etc.}

Modeling the POMDP Agent

- Transition function (T): In simple cases, we can assume that the state such as OS, whether ssh is installed or not, etc. are not changing and the transition for these actions are identity function. But, for actions such as breakPassword, we need to set the effectiveness of the method used becomes uncertainty in the effect of actions that we model in this transition function
- Observation function (Z): In simple cases, this is quite straightforward: The outcome of the commands
- Reward function (R): High positive when the system is exploited and small negative value for every action taken

Back to the problem…

- Autonomous pen-testing of a computer where uncertainty comes from not knowing:
  - The exact and full properties of the environment (aka the computer): This causes non-deterministic transition and possible error in observation
  - The strategy of the opponent (e.g., the sysadmin)
    - This is a difficult part
    - The agent's policy needs to consider the sysadmin strategy, the sysadmin strategy in turn needs to consider the agent's strategy, and the process repeats

The idea

- Actually, we only need to know the properties of the computer/network, so perhaps we don't need to explicitly represent the behavior of the sysadmin, but only represent the changes to the computer/network properties
  - We can represent the possible changes to the properties as a stochastic process and learn the parameters for this process during run-time
  - Interested to know more? http://rdl.cecs.anu.edu.au/papers/icaps20pomdp.pdf

This set of videos

- ✓ Part-1: Intro
  - ✓ Automated decision-making
- ✓ Part-2: Intro to POMDP
  - ✓ Framework for decision-making under uncertainty
  - ✓ Solving, aka. generating strategic decisions
- ✓ Part-3: Example of POMDP in Cyber security
  - ✓ Autonomous pen-testing