This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

A Game-Theoretic Risk Assessment Tool

A Short Demo

Stefan Schauer

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

2nd HyRiM End User Workshop

Barcelona, 15.11.2016

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Malware and Ransomware
- Percolation and Game Theory
- Demonstration of the Tool

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Malware and Ransomware
- Percolation and Game Theory
- Demonstration of the Tool

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Malware and Ransomware

- ICT systems are facing an increasing amount of infection and attacks by malware
  - Simple adware like DeskAd creating annoying content
  - Creation of bot networks for Distributed Denial-of-Service attacks (DDoS)
  - Complex ransomware like CryptoLocker to blackmail organizations
  - Some rootkits can also be used as a starting point to APT attacks

- Ransomware has the potential to cause a significant damage to an organization

- Even advanced measure like IDS or SIEM solutions are often not effective against malware attacks
  - Malware infection often relies on social engineering
  - Triggered by "soft factors" (e.g., phishing mails)
  - Propagation is possible over various ways (also including user interaction)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Malware and Ransomware

- Besides preventive actions it is important to assess the potential consequences of a malware infection
  - Especially utility providers operate highly sensitive networks
  - A failure of a small number of systems (or even a single system) might have significant effects
  - Damage can be caused to the organization as well as the population depending on the utility provider (societal effects)

- In HyRiM, we developed a novel framework for modeling and assessing the propagation of malware within a network
  - Framework is based on sound mathematical concepts
  - Special focus on the interconnection of different networks (ICT, SCADA, etc.)
  - Simulations are performed to obtain realistic data

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Malware and Ransomware
- Percolation and Game Theory
- Demonstration of the Tool

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Percolation Theory

- Infection of an ICT infrastructure with a malware can be seen similar to an infection of a biological system with a virus
  - One small part of the system becomes infected
  - This part then tends to infect his neighbors
  - Based on the strength of the system‘s defenses (immune system) the virus can propagate through the entire system

- In medicine, percolation theory is a standard framework to model the spread of epidemics
  - General assumption of a “homogenous outbreak”
  - Infection is equiprobable for any pair of nodes
  - Irrespectively of the nature of the two entities

- Percolation theory is rarely used in the field of security and risk management

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Percolation Theory

- Interconnected networks are not homogeneous
  - The probability of forwarding an error is not constant for each link
  - Highly dependent on the type of link between two nodes
  - Different types of connections have different probabilities of infecting their neighbor

- Percolation theory can be used to describe the propagation of failures in a network
  - Taking the "type" of a connection into account (not all failures are equally probable to propagate over a certain link)
  - Incorporating different probabilities of failure for each type
  - Taking interconnections (e.g., SCADA and utility network) into account
  - Taking cascading effects (how many nodes are "infected" after 2, 5, 10 time steps) into account

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Game Theory

- Goal is to define a mathematically sound framework for risk assessment
  - Special focus on interplay between IT, control and utility networks
  - Special focus on cascading effects and error propagation

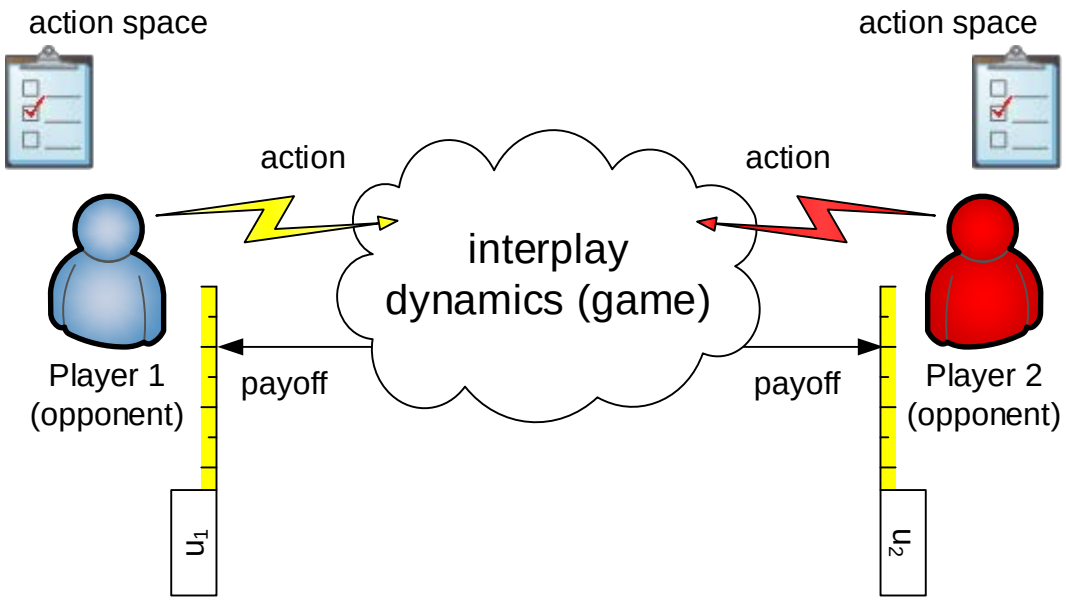
- Game Theory seems to be a very good candidate
  - Describes a competitive situation between two parties
  - Known and finite action space
  - Known, deterministic consequences determined by actions of all players
  - Gameplay with known rules and repeatable actions

- Problem: the setting for interconnected networks is not quite standard
  - External influences can occur (which are uncontrollable)
  - We have no information about the opponent's incentives and payoffs
  - We have random payoffs (instead of a single number)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Game Theory

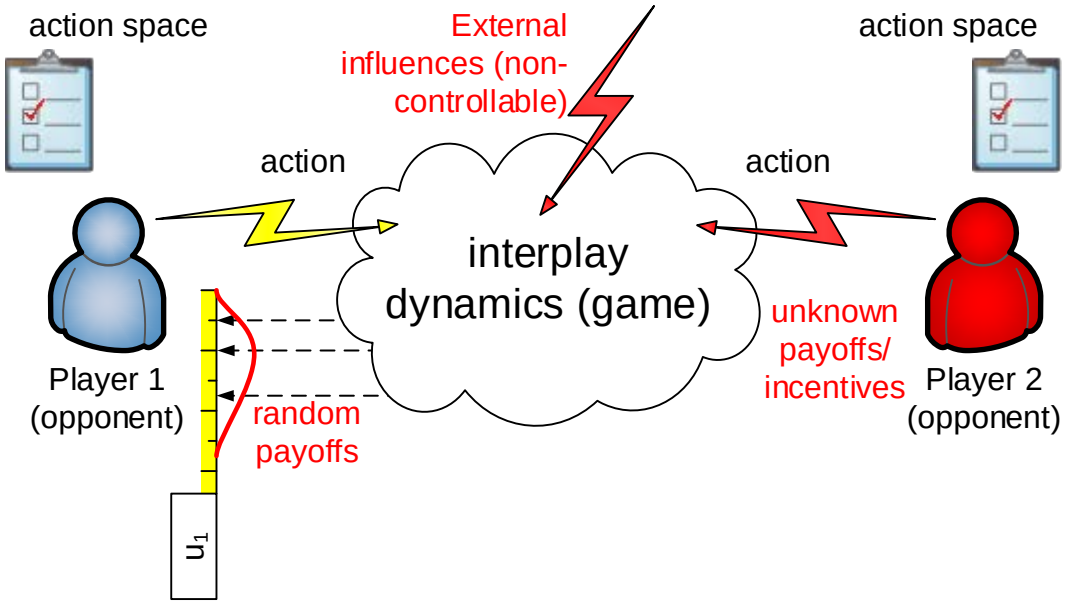
- In the general setting, two parties engage in a competitive situation
- Action space
  - Known
  - Finite
- Consequences
  - Known
  - Determined by actions of all players
  - Deterministic
- Gameplay
  - known rules/dynamics
  - Repeatable – players seek to maximise payoffs
- Solution: equilibrium = behavior that simultaneously maximizes the average payoffs for all players



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Game Theory

- In our approach, we engage in a competition against "the unknown"
- Action space
  - Known
  - Finite
- Consequences
  - Partially unknown
  - Determined by actions of all players
  - Stochastic
- Gameplay
  - (un)known rules
  - Repeatable – players seek to maximise payoffs
- Solution: define a series of actions (security strategy) with maximal payoff, no matter how the opponent behaves



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- Malware and Ransomware
- Percolation and Game Theory
- Demonstration of the Tool

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

A Game-Theoretic Risk Assessment Tool

A Short Demo

Stefan Schauer

stefan.schauer@ait.ac.at
AIT Austrian Institute of Technology
Lakeside B10a
9020 Klagenfurt
Austria

2nd HyRiM End User Workshop
Barcelona, 15.11.2016