Game Theory meets the Network Security Problem

Laura Gutierrez Funderburk

Ludwig-Maximilians-Universität München

July 2017

Contents

Motivation: What I find interesting about this problem

• Network security is a complex and challenging problem: explored for more than two decades, the security problem is far from solved.

• A key concept in game theory is the ability to examine a huge number of possible threat scenarios in the cyber system.

• Introducing information warfare: non-cooperative game between an attacker and a network administrator.

Taxonomy and Definitions

Game Theory:

1. Non-Cooperative Games

$\longrightarrow$ Static Games

$\longrightarrow$ Dynamic Games

2. Cooperative Games

The existing game-theoretic research as applied to network security falls under non-cooperative games.

Taxonomy and Definitions

Static Games
$\longrightarrow$ Complete Imperfect
$\longrightarrow$ Incomplete Imperfect
Dynamic Games
$\longrightarrow$ Complete Perfect
$\longrightarrow$ Complete Imperfect
$\longrightarrow$ Incomplete Perfect
$\longrightarrow$ Incomplete Imperfect

Furthermore games can either be Bayesian or Stochastic.

Existing Work

In this presentation I have chosen only two of the models I found the most interesting.

If you are interested in exploring different applications on this particular topic, refer to: [1] **A Survey of Game Theory as Applied to Network Security.** *Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, Qishi Wu*.

Static Games

Complete Imperfect Information

Jormokka et al. [2] introduced examples (information warfare scenario) of static games with complete imperfect information between network administrator and attacker.

Dynamic Games

Incomplete Imperfect Information

Alpcan et al [7] model interaction of an attacker and the network administrator as a repeated game with 'finite steps' or 'infinite steps'.

Models' Limitations

In reality a network administrator often faces a dynamic game with icomplete and imperfect information about the attacker. Current game models are limited in that they:

- Consider perfect information and assume defender is always able to detect attacks.
- Assume that the state transition probabilities are fixed before game starts.
- Assume player's actions are synchronous.
- Are not scalable with the size and complexity of the system under consideration.

Motivation for New Proposed Model

In addition to the limitations previously mentioned, these models assume network attacks are played only by a network administrator and an outside attacker, however in reality network users play an important role in the number of weaknesses introduced as users interact with the network and the network administrator on different levels.

Motivation for New Proposed Model

Data loss, data extraction and/or infected network:

(a1) Users who left network may have intentions to extract information
(a2) User neglicence: share passwords and keys; lose records or assets
(a3) Users employing personal computers for work, and not securing them properly

Motivation for New Proposed Model

Data loss, data extraction and/or infected network:

(b1) Users responding to outside attacks, i.e. phishing attacks
(b2) Users requesting admin access on their workstation and misusing it
(b3) Users trying to fix things themselves

Proposed Model: A first glance

What I propose is modeling a network attack as an information warfare game with three players and their objectives:

- Network administrator: wants to minimize attack instances and provide services to users.
- Outside attacker: wants to damage network via infection or information extraction.
- User: wants to use network to maximize results in his/her work. Network attacks are not in their interest.

Proposed Model: A first glance

Network administrator and outside attacker play a non-cooperative game, while the users play a wildcard and can either:

(1) Play a cooperative game with the network administrator
$\longrightarrow$ users + network administrator vs attacker,

(2) Play a non-cooperative game with the network administrator
$\longrightarrow$ users + attacker vs network administrator.

Remarks

• Ideally, network administrator and users play a cooperative game: network administrator provides services that users need to perform their work, without compromising network security.

• Delicate balance: a highly strong and secure network results in a network that is not user-friendly. Likewise, a network that is too easy to use might compromise security in a significant way.

Remarks

Users play a non-cooperative game with the administrator when they perceive him/her as an obstacle to their work, resulting in the following scenario:

- Users are more likely to miscommunicate issues
- Look for ways to gain control over workstations.
- Network becomes an easy target for outside attackers.

Goal: find strategies that will allow users and administrator to play a cooperative game, minimizing the probablity of a successful attack.

Questions?

References

[1] A Survey of Game Theory as Applied to Network Security. Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, Qishi Wu.
[2] J. Jormakka and J. V. E. Molsa. Modelling information warfare as a game. Journal of Information Warfare; Vol. 4(2),2005.
[3] T. Alpcan and T. Baser. A game theoretic analysis of intrusion detection in access control systems. Proc. of the 43rd IEEE Conference on Decision and Control, 2004.

Thank you for your attention!