Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense

Cheng Lei , Hong-Qi Zhang , Li-Ming Wang , Lu Liu , Duo-he Ma

PII: S0140-3664(17)30154-8
DOI: 10.1016/j.comcom.2017.12.001
Reference: COMCOM 5613

To appear in: *Computer Communications*

Received date: 9 February 2017
Revised date: 16 October 2017
Accepted date: 3 December 2017

Please cite this article as: Cheng Lei , Hong-Qi Zhang , Li-Ming Wang , Lu Liu , Duo-he Ma , Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense, *Computer Communications* (2017), doi: 10.1016/j.comcom.2017.12.001

Incomplete Information Markov Game Theoretic Approach to Strategy Generation for Moving Target Defense

Cheng Lei[1,3], Hong-Qi Zhang[1,3], Li-Ming Wang[2], Lu Liu[1,3], Duo-he Ma[2]

[1.] *China National Digital Switching System Engineering & Technological Research Center, Zhengzhou Henan Province 450001, China;*

[2.] *State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China;*

[3.] *Henan Key Laboratory of Information Security, Zhengzhou Henan Province 450001, China*

Abstract: With the extensively study on moving target defense, optimal strategy generation has become one of the key problems in current research. A novel of incomplete information Markov game theoretic approach to strategy generation for moving target defense is proposed to solve the existing problems. On the one hand, traditional matrix game structure and complete information assumption often fail to describe moving target defense confrontation accurately. To deal with this inaccuracy, moving target defense game model based on incomplete information Markov game theory is constructed by introducing moving attack surface and moving exploration surface concept, extending optimal strategy selection of moving target defense with incomplete information from mono-state or mono-phase to multi-stated and multi-phased. On the other hand, traditional models care little about defense cost in the process of optimal strategy generation. After comprehensively analyzing the impact of defensive cost and defensive benefit on strategy generation, an optimal strategy generation algorithm is designed to prevent the deviation of the selected strategies from actual network conditions, thus ensuring the correctness of optimal strategy generation. Finally, simulation and deduction experiments have been performed in a case study so as to confirm the feasibility and the effectiveness of the proposed approach.

Key words: Moving Target Defense; Incomplete Information; Markov Game; Optimal Strategy Generation; Moving Attack Surface; Moving Exploration Surface

0. Introduction

Nowadays, more and more network attacks, such as SWIFT bank attack and Autonomous System Prefix hijacking challenges the network security by using either known vulnerabilities or unknown vulnerabilities (zero-day). Adversarial dynamics is one of the critical facets within network security challenges. While defender leverages capabilities to minimize the potential impact of attack, attacker simultaneously develops countermeasures to the observed defenses. Network security is facing "unbalance of offense and defense" challenges seriously. Generally speaking, the main problems are as follows: a) The security vulnerabilities are inevitably, leading to information asymmetry. Attacker can install customized backdoors to control and threaten network systems by exploiting network resource vulnerabilities. Defender is hard to explore all possible vulnerabilities based on prior knowledge. b) The certainty and the static structure of existing network systems provides necessary conditions for cyber kill-chain implementation, leading to time asymmetry. Attacker can scan and collect information on targeted systems with sufficient time. The defensive methods based on threat characteristics and security vulnerabilities usually lag behind attackers' exploitation of system vulnerabilities. c) What's more, the isomorphism of network architecture aggravates the unbalance in cyber security. Attacker can implement cost-effective attacks by using similar vulnerabilities in different network components. While