Accepted Manuscript

Stackelberg games for modeling defense scenarios against cloud security threats

Agnieszka Jakóbik, Francesco Palmieri, Joanna Kołodziej

PII: S1084-8045(18)30066-3

DOI: 10.1016/j.jnca.2018.02.015

Reference: YJNCA 2074

To appear in: *Journal of Network and Computer Applications*

Received Date: 1 June 2017

Revised Date: 8 February 2018

Accepted Date: 27 February 2018

Please cite this article as: Jakóbik, A., Palmieri, F., Kołodziej, J., Stackelberg games for modeling defense scenarios against cloud security threats, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.02.015.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Stackelberg Games for Modeling Defense Scenarios Against Cloud Security Threats

Agnieszka Jakóbik*

Institute of Computer Science Cracow University of Technology, Poland

Francesco Palmieri*

Department of Computer Science, University of Salerno, Italy

Joanna Kołodziej*

Research and Academic Computer Network (NASK) Kolska st 12, 01-045 Warsaw, Poland

Abstract

Stackelberg games may reveal to be extremely useful in supporting decisions in attack-defense scenarios. We call such games Security Stackelberg games. They are characterized by two kinds of players: the defender, who defines his strategy in advance, and the attacker, who follows the defender's decisions. Security Stackelberg games may be used to model a typical cloud security scenario, where the provider has to expose its defense strategy and the attackers act by following the provider's actions. In this work we define a model based on Stackelberg games that enables the automatic selection of provider-level security decisions in Cloud Computing environments. Potential Cloud attack scenarios are modeled as nonzero-sum Security Stackelberg games between the attacker and the Cloud provider. This allows the estimation of the strategy that minimizes the reward for the attacker and maximizes the gain of the defender. The model has been experimentally verified to be effective in automatically determining defense strategies from the cloud provider perspective.

Keywords: Cloud Security; Game Theory; Stackelberg Games; Modeling

*Corresponding author
Email address: agneskrok@gmail.com (Agnieszka Jakóbik)

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات