Computer Science Review 26 (2017) 1–16

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Survey

A survey on the usability and practical applications of Graphical Security Models

Jin B. Hong [a],*, Dong Seong Kim [a], Chun-Jen Chung [b], Dijiang Huang [b]

[a] *Department of Computer Science and Software Engineering, University of Canterbury, New Zealand*
[b] *Department of Computer Science, Arizona State University, USA*

HIGHLIGHTS

- Describe the development of security models and their current functions.
- Classify the applications of existing security models.
- Compare the scalability of security models with respect to the complexity analysis.
- List the use of security metrics, available tools and network domains applicable.
- Discuss the future directions of security models.

ARTICLE INFO

Article history:
Received 1 July 2016
Received in revised form 1 September 2017
Accepted 1 September 2017

Keywords:
Attack graphs
Attack trees
Security analysis
Security metrics
Security models

ABSTRACT

This paper presents and discusses the current state of Graphical Security Models (GrSM), in terms of four GrSM phases: (i) generation, (ii) representation, (iii) evaluation, and (iv) modification. Although many studies focused on improving the usability, efficiency, and functionality of GrSMs (e.g., by using various model types and evaluation techniques), the networked system is evolving with many hosts and frequently changing topologies (e.g., Cloud, SDN, IoT etc.). To investigate the usability of GrSMs, this survey summarizes the characteristics of past research studies in terms of their development and computational complexity analysis, and specify their applications in terms of security metrics, availability of tools and their applicable domains. We also discuss the practical issues of modeling security, differences of GrSMs and their usability for future networks that are large and dynamic.

Contents

* Corresponding author.
E-mail addresses: jho102@uclive.ac.nz (J.B. Hong), dongseong.kim@canterbury.ac.nz (D.S. Kim), chung-jen.chung@asu.edu (C.-J. Chung), dijiang@asu.edu (D. Huang).

https://doi.org/10.1016/j.cosrev.2017.09.001
1574-0137/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

It is of paramount importance to understand how secure a networked system is to prevent damages caused by cyber attacks. A widely adopted method is to use a Graphical Security Model (GrSM), (e.g., an Attack Graph (AG) [1] or an Attack Tree (AT) [2]) to assess the security of a given networked system and to recommend security hardenings. AGs are one of the basic structures for most graph-based GrSMs, and ATs are one for most tree-based GrSMs. To address the limitations of AGs and ATs, new GrSMs are proposed (e.g., Attack Defense Tree [3]) to enhance the security assessment capabilities, and Hierarchical Attack Representation Models [4] using hierarchy features to improve the scalability. As a result, there is a wide range of different GrSMs available today [5], but they do not necessarily provide the same security analysis nor functions. Consequently, a diverse family of GrSMs exists today that creates a difficulty for users to determine the most suitable one for the security analysis of their networked systems.

To cope with various features of GrSMs, surveys are conducted to reflect their efficiencies in many aspects (e.g., generation, evaluation, and their complexities). However, the focuses of those surveys have changed over the years due to various reasons, such as a development of networks (e.g., static networks to dynamic networks such as cloud networks), and also the availability of tools (e.g., NetSPA [6], MulVAL [7] and NAVIGATOR [8]). Lippmann and Ingols [9] focused on the scalability of GrSMs when generating them, where prior to this survey there were no GrSMs that have analyzed more than 20 hosts in a networked system. The survey conducted by Khaitan and Raheja [10] on the same topic (i.e., scalability of GrSMs) reported the poor scalability as well. On the other hand, Alhomidi and Reed [11] conducted a survey based on the representation of graph-based GrSMs, where structure of an AG can be represented differently based on different features implemented (e.g., clustering (MPAG) and non-clustering (AG)), but there is no standard model to cover all these features. Kordy et al. [5] conducted a survey based on directed acyclic graphs