SpringerBriefs in Computer Science

Series Editors

For further volumes:
http://www.springer.com/series/10028

Suguo Du • Haojin Zhu

Security Assessment in Vehicular Networks

Springer

Suguo Du
Antai College of Economics
and Management
Shanghai Jiao Tong University
Shanghai
People's Republic of China

Haojin Zhu
Department of Computer Science
and Engineering
Shanghai Jiao Tong University
Shanghai
People's Republic of China

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4614-9356-3 ISBN 978-1-4614-9357-0 (eBook)
DOI 10.1007/978-1-4614-9357-0
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013951520

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To my parents

Preface

Vehicular Networks, or Vehicular Ad-hoc Networks (VANETs), is regarded as a promising approach for future intelligent transportation system, and enables a wide range of safety and Infotainment applications. From the safety perspective, the introduction of VANETS greatly increases the safety of passengers by exchanging safety relevant information. From the Infotainment perspective, it exploits the Vehicle-to-vehicle communications and Vehicle-to-Road Side Unit communications to allow ubiquitous Internet Access, Video Streaming, Location-based Service, Content Distribution and Traffic Monitoring. The security and privacy is more than critical for the success of vehicular networks.

This book is designed to introduce some methods such as attack tree, attack-defense tree and attack-defense game from a system view for analyzing the vehicular network security and privacy problems. The existing research on VANETs security and privacy mainly focuses on the preventive techniques. From a system point of view, it lacks a comprehensive yet well-defined security evaluation to allow the system administrator to identify the most critical security threats and thus determine the appropriate defense strategy, which are more than important for the overall success of VANETs deployment. The existing risk analysis schemes include attack tree, attack graph or defense tree based solutions. However, there are several research challenges which make the existing security analysis solutions cannot work well for security and privacy evaluation in VANETs. Firstly, for VANETs security, the defense strategy is directly correlated to the attack strategy and vice versa, which means that the security evaluation should consider both of attack and the defense side rather than any single one. Secondly, most of the existing security solutions only consider how to prevent an attack while fail to consider the costs and gains of the attacker and the defender. In reality, a rational attacker or defender may try to maximize its attack or defense benefits instead of blindly launching an attack or adopting a countermeasure. Lastly, but no less importantly, how to model the mutual interaction between the attacker and defender remains a great challenge for VANETs security evaluation.

This book presents several novel approaches to model the interaction between the attacker and the defender and assess the security of the considered VANETs. The first security assessment approach presented in this book is based on attack tree

security assessment model, which leverages tree based method to model and analysis the risk of the system and identify the possible attacking strategies the adversaries may launch. With the help of the attack tree model, it is convenient to analyze the capability of the attack source and estimate the degree or the impact a certain threat might bring to the system.

To further capture the interaction between the attacker and the defender, we further propose to utilize the attack-defense tree model to express the potential countermeasures which could be used to mitigate the system. The difference between an attack tree and an attack-defense tree is that the front only represents the attack strategies that attackers can launch, while the latter includes the set of countermeasures which can mitigate the possible damages produced by the attackers.

By considering rational participants that aim to maximize their payoff function, we propose a game-theoretic analysis approach to investigate the possible strategies that the security administrator and the attacker could adopt. On one side the VANETs security administrator wants to protect the security of the vehicular networks by adopting countermeasures to thwart the attacks; on the other side, the attacker wants to exploit the vulnerabilities and obtain some profit by attacking the vehicular networks. However, they cannot maximum their utility at the same time because one's action that aims to increase its own benefits will reduce its adversary's utility. Under this setting, we discuss the potential strategies of the defender and the attacker by modeling it as an attack-defense game. We then give a detailed analysis on its Nash Equilibrium.

Since many real world systems operate in multiple phases and, for mission success, all phases must be completed without failure. In practice, the attack strategy will evaluate from simple attack to more advanced yet complicated attacks along with the evolution of the defense strategy. Therefore, defending the attack succeeds if and only if the defense of all of phases succeed. We introduce a phased attack-defense game to model the interactions between the attacker and defender for VANET security assessment.

This book can be used for graduate students who interest in network security and privacy research area in their first year's literatures reviewing phase. This book can be a reference reading material for management science or computer science graduate students. The main mathematical prerequisite are the rudiments of Boolean algebra and game theory.

Finally we would like to thank Mr. Xiaolong Li and Mr. Junbo Du for their devotion to this work.

Shanghai, People's Republic of China — Suguo Du
August 2013 — Haojin Zhu

Contents

1 Introduction to Vehicular Networks Security 1
1.1 Vehicular Networks 1
1.2 Applications in Emerging Vehicular Networks 2
1.3 Security Requirements for Emerging Vehicular Networks 3
1.4 Vehicular Security: State-of-the-Art 5
1.5 System Model 7
1.6 Summary 7

2 Security Assessment via Attack Tree Model 9
2.1 Introduction of Privacy Protecting in VANETs 9
2.2 Attack Tree Model for VENET Privacy 10
2.3 Risk Assessment 12
2.4 Attack Scenarios 15
2.5 Summary 16

3 Attack-Defense Tree Based Security Assessment 17
3.1 Introduction to Attack-Defense Tree Model 17
3.2 Building Attack-Defense Tree for VANETs Security 18
3.3 Introduction of ROI and ROA for Attack-Defense Tree 20
3.4 Summary 22

4 A VANETs Attack-Defense Game 23
4.1 Game Model 23
4.2 Equilibrium Concepts 24
4.3 Security Analysis of Attack-Defense Game: A Case Study 29
4.4 Summary 34

5 Modelling of Multiple Phased Attack on VANET Security 35
5.1 System Architecture 35
5.2 A Phased Attack-Defense Game for VANETs 37
5.2.1 Game Model 38
5.2.2 Main Solutions 40
5.3 Summary 42

Glossary 43

References 45

Index 49

Acronyms

AAA	Authentication, Authorization and Accounting
ALE	Annual Expected Loss
CA	Certificate Authority
CI	Cost of Investment
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
EBL	Extended Brake Lights
ECDSA	Elliptic Curve Digital Signature Algorithm
GI	Gain of Investment
ILD	Inductive Loop Detectors
MAC	Medium Access Control
OBU	On Board Unit
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
ROA	Return On Attack
ROI	Return on Investment
RM	Risk Mitigation
RSUs	Road Side Units
TLS	Transport Level Security
VANETs	Vehicular Ad-hoc Networks
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle