SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Jie Yang • Yingying Chen • Wade Trappe
Jerry Cheng

Pervasive Wireless Environments: Detecting and Localizing User Spoofing

Springer

Jie Yang
Department of Computer Science and Engineering
Oakland University
Rochester
Michigan
USA

Yingying Chen
Department Electrical & Computer Engineering
Stevens Institute of Technology
Hoboken
New Jersey
USA

Wade Trappe
Wireless Information Network Lab
Rutgers, The State University
of New Jersey
North Brunswick
New Jersey, USA

Jerry Cheng
Rutgers, The State University
of New Jersey
New Brunswick
New Jersey
USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-3-319-07355-2 ISBN 978-3-319-07356-9 (eBook)
DOI 10.1007/978-3-319-07356-9
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014940861

Printed on acid-free paper

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

Preface

As more wireless and sensor networks are deployed, information provided and shared by wireless systems has become an inseparable part of our social fabric. However, wireless security is often cited as a major technical barrier that must be overcome before widespread adoption of wireless information systems. Due to the shared nature of the wireless medium, adversaries can gather useful identity information during passive monitoring and further utilize the identity information to perform user spoofing. During an user spoofing attack, an adversary can forge its identity to masquerade as another device, or even creates multiple illegitimate identities in the networks. For instance, in Wi-Fi network, it is easy for an attacker to modify its MAC address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point or as an authorized client, an attacker can launch denial of service attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

Attacks originated from user spoofing will have a serious impact on the successful deployment of pervasive wireless environments. It is thus desirable to detect the presence of user spoofing and eliminate it from the network. The traditional approach to prevent user spoofing is to apply cryptographic authentication. However, authentication requires additional key management infrastructural overhead and extra computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available on the wireless devices and the dynamics introduced by the node mobility, it is not always possible to deploy authentication. This book provides a different approach by using the physical properties associated with wireless transmissions to detect the presence of user spoofing. The book begins by introducing user spoofing in wireless networks, presenting the motivation of the book and summarizing our contributions of the book. After that, we discuss the feasibility of launching user spoofing attacks and their impact on the pervasive wireless environments in Chap. 2. In Chap. 3, we describe the attack detection model that exploits the spatial correlation of Received Signal Strength (RSS) inherited from wireless devices as a foundation. This chapter further presents the performance evaluation of the spoofing attack detection model through experiments in practical environments. In Chap. 4, we deal with the situation when multiple

spoofing attackers are present. We develop a statistical approach to determine the number of attackers, and further show how to localize these adversaries. Both the attacker number determination and adversaries localization methods are evaluated though two wireless testbeds including both Wi-Fi and Zigbee networks. In Chap. 5, we study user spoofing under mobile wireless networks. For many people, mobile devices are becoming the favored portal to their online social lives. Thus, the identity fraud conducted by malicious mobile agents will have detrimental impact on the successful deployment of mobile pervasive applications. We develop the DEMOTE system, which exploits the correlation within the RSS trace based on each devices identity to detect mobile attackers in Chap. 5. The DEMOTE system is evaluated in an office environment in both Wi-Fi and Zigbee networks. In Chap. 6, we provide an overview of the state-of-the-art research. Finally, the conclusions and future directions are presented in Chap. 7.

Contents