SpringerBriefs on Cyber Security Systems and Networks

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies. It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook. It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The mainly focuses on the following research topics:

Fundamentals and Theories

- Cryptography for cyber security
- Theories of cyber security
- Provable security

Cyber Systems and Networks

- Cyber systems security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

Applications and Others

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at http://www.springer.com/series/15797

Bo Liu · Wanlei Zhou · Tianqing Zhu
Yong Xiang · Kun Wang

Location Privacy in Mobile Applications

Springer

Bo Liu
La Trobe University
Bundoora, VIC, Australia

Wanlei Zhou
School of Software
University of Technology Sydney
Ultimo, NSW, Australia

Tianqing Zhu
School of Software
University of Technology Sydney
Ultimo, NSW, Australia

Yong Xiang
School of Information Technology
Deakin University
Burwood, VIC, Australia

Kun Wang
School of Internet of Things
Nanjing University of Posts
and Telecommunications
Nanjing, China

ISSN 2522-5561 ISSN 2522-557X (electronic)
SpringerBriefs on Cyber Security Systems and Networks
ISBN 978-981-13-1704-0 ISBN 978-981-13-1705-7 (eBook)
https://doi.org/10.1007/978-981-13-1705-7

Library of Congress Control Number: 2018953315

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The Global Positioning System (GPS) module has almost become standard in mobile phones in recent years, driving the growth of location-based services (LBSs) which provide a variety of information services (such as mobile social networks, navigation, places of interest finding, sports and healthy assistant, augmented reality games) based on the location data. As all the LBS providers require the access permission to users' location data, severe privacy concerns are raised at the same time. Therefore, effective location privacy preservation is foremost for these mobile applications.

Despite the big amount of papers in this area, there lacks a systematic study to present all related components of the problem. Moreover, the gap between theory and practice is big. To overcome these obstacles, this book will provide an integrated five-element framework for location privacy research, which includes analysis of location privacy definitions, attacks and adversaries, location privacy protection methods, location privacy metrics, and location-based mobile applications. In addition, we analyze the relationships between the different elements of location privacy. For example, a particular attack is targeted to the location data in a particular application. Then, it can be prevented by a certain type of protection method. Moreover, location privacy will be studied in detail in three different applications. We will also share some insights on the possible research directions.

We believe that this study will shed light on the research issues of location privacy and promote the advance and development of future location-based mobile applications. The content will be useful for researchers, students, and engineers in this area.

Melbourne, Australia — Bo Liu
June 2018

Contents

Acronyms

AR	Augmented reality
DP	Differential privacy
DSRC	Dedicated short-range communication
GPS	Global positioning system
LBA	Location-based application
LBS	Location-based service
LPPM	Location privacy preservation mechanism
MCS	Mobile crowd sensing
MSN	Mobile social network
OBU	On-board unit
PIR	Private information retrieval
POI	Place of interest
PSD	Personal sensing device
QoS	Quality of service
RoT	Region of Task
RSU	Roadside unit
SP	Service provider
SQL	Service quality loss
TTP	Trusted third party
V2R	Vehicle-to-roadside
V2V	Vehicle-to-vehicle
WAVE	Wireless Access for Vehicular Environments