Securing Emerging Wireless Systems

Lower-Layer Approaches

Yingying Chen • Wenyuan Xu • Wade Trappe •
YanYong Zhang

Securing Emerging Wireless Systems

Lower-Layer Approaches

Springer

Yingying Chen
Stevens Institute of Technology
Hoboken, NJ
USA

Wenyuan Xu
University of South Carolina
Columbia, SC
USA

Wade Trappe
Rutgers University
North Brunswick, NJ
USA

Yanyong Zhang
Rutgers University
North Brunswick, NJ
USA

ISBN 978-0-387-88490-5 e-ISBN 978-0-387-88491-2

Library of Congress Control Number: 2008936474

Printed on acid-free paper.

springer.com

To Our Families

Preface

We live in an increasingly wireless world and, even though the benefits of tetherless communication are sure to attract a plethora of new applications and help bring communication to those who were never before connected to the broader world, these very same benefits can also serve as the means to cause damage upon individuals, enterprises and governments. Unlike traditional wired communication, where physically protecting the medium is, to a large part, possible by running cables underground and wires in walls, wireless communication is not able to physically protected in the conventional sense. Sure, wireless access points are placed in buildings that may be locked, or cellular basestations are protected by fences and security cameras, but the medium itself is trivially open to a broad array of threats and thus securing wireless communication necessitates a collection of tools that can suitable protect the wireless medium.

This book is about security for wireless networks. However, whereas most conventional approaches to security focus on *cryptographic* solutions that are applied in building families of interconnected network security protocols, this book instead focuses on complementary techniques that aim to invoke unique properties of wireless communications in order to add security to wireless systems.

In order to place this book in an appropriate context, it is perhaps best to think of a simple analogy. Consider a cocktail party where two people, Alice and Bob in the usual parlay of the security community, are trying to have a conversation. Their vocal chords create an audio waveform that travels through the air and which can be heard by others who are close enough to Alice and Bob. Their voices correspond to wireless communication signals,

which propagate in all directions. If Alice and Bob want to make certain that there are no eavesdroppers, they must communicate in a way to make certain that others won't be able to hear or decipher their conversation. Another concern that they might have is that there may be an imposter in the room, seeking to imitate Alice, when starting a conversation with Bob. For such masquerading or spoofing attacks, Bob must use some information specific to Alice, such as her previous location or even some unique aspect of her voice, in order to discern between legitimate and illegitimate conversations. Or, yet another concern that Alice and Bob may have is that there may be unsociable people present at the party who constantly interrupt their conversation. In such cases, Alice and Bob must find a way to excuse themselves and resume their conversation at a different place.

In this book, we deal with these sort of challenges as they apply to wireless communication networks. When considering the standard protocol stack, the aspects that are unique to wireless communications exist at the lower layers of the network stack. Signals and their properties are representative of the physical layer, and take on special characteristics based on their location relative to other wireless devices and to the background environment. It is at the lowest layer of the protocol stack where transmitter location has its greatest impact. The link layer, or medium access control (MAC) layer, must cope with the fact that multiple communications (or conversations) might be carried on at the same time and, just as we have *social protocols* that govern our interactions with each other in a party, wireless networks must also employ suitable MAC protocols to allow for sharing of the wireless medium. Although all communications systems involve localized communications as the basic building block to communicating long distances, many different wireless systems, ranging from sensor networks to ad hoc networks, are characterized by their multi-hop routing protocols. It is at the routing layer where we may direct communication towards or away from certain areas in hopes of achieving improved security or privacy.

Throughout this book we will explore a variety of different *lower layer* strategies for securing wireless networks. Our solutions build largely upon non-cryptographic methods, though occasionally we will employ cryptography in our solutions to make them more robust and resilient to attacks. Applications of cryptography to securing wireless protocols is a necessary component to securing wireless systems, and we thus feel it is important to iterate up front that the methods presented in this book should not be considered a replacement to a well-designed network security protocol. The methods presented in this book will never replace the role of TLS or HTTPS. Instead, it is our viewpoint and belief that wireless systems can only be secured when the full spectrum of tools available to the wireless engineer are brought to bear on the problem. A toolbox that leaves out either cryptography or lower layer characteristics would correspond to an incomplete set of tools that might require more effort in order to achieve

a comparable level of security when cryptography and lower layer security methods are combined.

The approaches to securing wireless systems that exploit lower layer phenomena is an emerging area of research in the wireless security community, and the material presented in this book is, in large part, a compilation of research that was conducted by the authors. However, there are many people who should be acknowledged for their efforts in conducting research that led to some of the material presented in the book. Notably, the authors would like to acknowledge their colleagues Qing Li, Pandurang Kamat, Shu Chen, and Zang Li, who conducted research on forge-resistant relationships, privacy-enhanced routing, and physical layer security as part of their thesis research. Additionally, the authors would like to acknowledge several other collaborators who have helped in different ways to make this research lively: Konstantinos Kleisouris, Eiman Elnahraway, John-Austin Francisco, Rob Miller, Ke Ma, Richard Martin, Rich Howard, and Ivan Seskar. Each, in their own way, has helped make the material presented in this book possible.

Contents