Preface

Over the past few decades, the role of computing has grown from being used mainly for scientific purposes, into being part of our everyday life, where it is used for purposes such as communication, entertainment, and device control in the state-of-the-art consumer products. The ubiquity of communication networks is facilitating the development of wireless and Internet applications aimed at allowing users to communicate and collaborate amongst themselves. Soon, group-oriented services will be customary-they will be essential for increasing productivity in the future workplace, and they will be integral to how we redefine our sense of community. Ultimately, these group-oriented services will be heterogeneous in nature, bringing together a diverse clientele of users with varying amounts of computing power and communication capabilities. However, before these group-oriented services can materialize, technologies must be developed to guarantee that the information and data exchanged in these group-scenarios are protected. In short, it is necessary to develop solutions that will make multi-user services trustworthy and secure.

Recently computing and networking research has shifted from the static model of the wired Internet towards the new and exciting "anytime-anywhere" service model of the mobile Internet. At the heart of the technologies facilitating such pervasive computing are recent advancements in wireless technologies that will provide the ubiquitous communication coverage that is so coveted by mobile services. Moreover, due to the fact that wireless devices can seamlessly blend into users' lives, it is easy to predict that future wireless networks will gradually become the primary interface for consumer applications. These group-oriented services will be popular as they will be

essential for increasing productivity in the future workplace. Already the migration to mobile computing has started, and it appears that the market for mobile services, or "m-commerce", will succeed as recent estimates project m-commerce to grow to involve over 1 billion subscribers. In spite of the predicted success of the wireless market, there are several disruptive challenges lurking in the future that threaten the successful adoption of wireless services. Perhaps core amongst these challenges are two issues, namely, platform heterogeneity, and secure and trusted communications.

The first issue points to the fact that wireless systems appear to be shifting away from the single-platform model of the 1990's to a free-for-all mixture of technologies battling it out in unlicensed bands of spectrum. Even the broad umbrella of Beyond-3G and 4G systems, along with forward-planning 3G/WLAN interworking solutions, do not appear to be positioned to capture the broad heterogeneity that will be introduced when completely new classes of wireless systems, such as cognitive radios, mesh networks, and wireless personal area networks are deployed using newly-developed programmable radio technologies. Further, it can be expected that a diverse array of new media services will drive the mobile Internet, and new multimedia delivery devices, such as wireless audio-visual devices and the next evolution of wearable computing devices, will emerge as important new products complementing today's laptop computers and personal digital assistants, providing a revolutionary means to communicate and collaborate from anywhere at anytime.

The second hurdle facing wireless systems is security. Even for the existing wireless networks, security is often cited as a major technical barrier that must be overcome before widespread adoption of mobile services can occur. The increasingly popular "WiFi" or 802.11 wireless local-area network was initially based on a standard with relatively weak wireless security called WEP, resulting in major security concerns as the equipment was deployed in offices and homes. Further, emerging 3G cellular data services also have limited security capabilities. Moreover, it has become clear that end-to-end security solutions, which were originally designed for the wired Internet, have limited applicability to the unique problems associated with wireless networks. Add to this the foreseeable heterogeneity in devices and user profiles that emerging wireless networks will introduce, and it is evident that there is a need for research targeted at developing security solutions for next-generation mobile services.

One of the most suitable technologies for delivering data to groups of users is multicast networking. Multicasting has seen significant advancements recently, in both the underlying technology as well as the deployment of applications utilizing multicast technologies. Already there are multicast services that stream stock quotes, and provide video and audio on demand. The adaptation of multicast into commercial applications requires security functionalities, such as authentication, non-repudiation, and access control. Of these, access control is paramount as it is the first line of defense needed

to protect the value of an application's data. A service provider may control access to content by encrypting the content using a key that is shared by all group members. The problem of access control becomes more difficult when the content is distributed to a group of users since membership will most likely be dynamic, with users joining and leaving the service for a variety of reasons, and therefore necessitating the ability to update keys.

Key management is accomplished either by using a centralized entity that is responsible for distributing keys to users, or by contributory protocols where legitimate members exchange information to agree upon a key. Typical group key management schemes seek to minimize either the amount of rounds needed in establishing the group key, or the size of the messages, and treat all users as identical. However, these approaches do not factor in the varying requirements of the users, the underlying network, or the application, and are therefore not well suited to provide solutions efficient for all users, for all networks, or for all types of applications. In particular, since many applications will involve a heterogeneous clientele consisting of group members with different computational capabilities, pricing plans, and bandwidth resources, these network-aware factors must be considered when designing an access control system.

The pervasiveness of computing has made it increasingly difficult to find any aspects of computing that are unaffected by issues from the underlying application and communication network. Applications must consider the requirements of the users and the underlying network conditions in order to provide a service that meets the demands of as many users as possible. A similar approach is needed for designing the security architecture for an application. In order to secure tomorrow's computing systems, it is essential to develop a network-aware framework that provides trustworthiness by jointly considering issues of computing and communications in dynamic, heterogeneous group environments.

Wireless multicasting will support many new multimedia applications, ranging from the broadcasting of media content for entertainment services, to video surveillance for remote monitoring applications, to multiparty "on-the-go" collaborations that will increase our productivity. Securing the next wave of wireless communications will require new strategies since traditional multicast security solutions are not targeted at addressing issues specific to emerging new applications such as wireless multimedia multicast services.

Before group-oriented wireless services can materialize, technologies must be developed to guarantee that the information and data exchanged are protected. In short, it is necessary to develop solutions that will make wireless multi-user multimedia services trustworthy and secure in the diverse wireless networks of the future. In order to accomplish this we have to have a better understanding with a holistic view of security solutions that address the following three topics:

- Access Control and Data Confidentiality serve as the first line of defense needed to protect the value of an application's data. A service provider may control access to content by encrypting the content using a key that is shared by all group members. The problem of access control for multicasts is challenging since group membership will most likely be dynamic, with users joining and leaving-necessitating the ability to update keys. However, traditional multicast key management schemes do not factor in the varying requirements of the users, the underlying network, or the application, and therefore are not adequately efficient for wireless multimedia multicast services.

- Service Authentication and Verification are important security issues for the media service. Traditional public key authentication is not suitable for wireless networks since many mobile devices will be low-powered, with limited computational and storage resources. Additionally, the strict delay requirements of multimedia data prevent popular delayed key disclosure techniques from being appropriate for wireless multimedia services. Together, these requirements necessitate the development of new classes of delay-sensitive authentication mechanisms for multimedia multicasting. An additional issue that is relevant for service validation is non-repudiation. Although non-repudiation is not typically studied in the context of multicast services, it is of particular importance for multimedia multicast services since the combination of advanced compression coding and best-effort wireless multicasting will not provide any guarantee of the quality of service delivered. It is important to both the service provider and the customers that mechanisms are available to irrefutably prove the quality of service delivered during a multimedia multicast service.

- Attack and Immunization Countermeasures are part of the security design cycle. The development of a suite of security protocols should involve an active phase of attacking the protocols in the suite as well as other protocols. The lessons learned by this effort give valuable insight into strengthening, or immunizing, the protocols to different types of attacks.

Throughout the discussion of these topics in this book, we take the viewpoint that the combination of content and wireless infrastructure introduces unique challenges that are not adequately addressed by generic multicast security solutions. This book presents the research results that have been undertaken by the authors in the past decade on security and reliability issues of group-based computing and communications. We hope our articulating point of the book– the network-aware approach toward security of group communications– can serve as an enlightening view for future development of wireless security.

Finally, we would like to acknowledge the assistance of the Army Research Office, whose University Research Initiatives has helped support the investigations behind many of the results that we present in this book. Additionally, we would like to express our thanks to the many people who have helped us in developing this book, including Yinian Mao, Min Wu, Yinian Mao, Jie Song, Wei Yu, and Qing Li.

http://www.springer.com/978-0-387-68846-6

Network-Aware Security for Group Communications
Sun, Y.; Trappe, W.; Liu, K.J.R.
2008, XVIII, 304 p., Hardcover
ISBN: 978-0-387-68846-6