Secure Wireless Networking

Adrian Perrig, Wade Trappe, Virgil Gligor, Radha Poovendran, and Heejo Lee

Wireless technologies have had a significant impact on computing and communication technologies in the past decade, and we are thus now progressing to the new "anytime-anywhere" service model of the mobile Internet. Unfortunately, the affordability and availability of wireless technologies that makes them so attractive, also makes them an enticing target for security threats. As new wireless technologies continue to emerge, many of which will be highly flexible and programmable (such as the next generation of software radios), it will be easier than ever before for adversaries to acquire the equipment and the means to launch new security or privacy attacks.

The challenge facing the security community is to achieve security in spite of the fact that the wireless medium is an open "broadcast" medium, in spite of the fact that wireless devices are affordable and increasingly programmable, in spite of the fact that in a mobile environment security associations must be made when no trust relationships existed previously. Thus, the challenges associated with ensuring the trustworthy and private operation of wireless systems is a significant challenge that requires new techniques that build upon traditional security mechanisms.

The intent of this special issue is to focus on the exchange of cutting-edge research in security for new wireless systems (e.g. cognitive radios, RFID, industrial control systems, and vehicular networks), as well as the privacy issues associated with these emerging technologies. As editors of this special issue, we saw many exciting papers cross our desks and had the tough challenge of selecting a subset of these papers that carried the spirit of our vision for what constitutes the cutting-edge of wireless security. Among twenty eight submissions, we selected eleven papers to be included in this special issue. After looking over the papers, we found that three dominant themes emerged:

- Lower-layer Approaches to Securing Wireless Networks
- Security and Privacy for Emerging Networks
- Security and Formal Methods for Wide Area Wireless Networks

This special issue has been divided into three sections according to these themes, and each section includes a collection of papers that we and our reviewers found to be exciting.

We have chosen the first section to include papers on lower-layer approaches to securing wireless networks. The features that most differentiate wireless networks from other networks reside at the lower layers of the protocol stack. When one thinks of the physical layer for a wireless network, very unique properties arise, such as fading phenomena or the broadcast nature of the medium or the irregularity of radio propagation. It is precisely the physical and medium access layers of wireless communication that gives an adversary so much power. Unlike wired media, where listening on communications requires tapping a wire (an endeavor that can usually be thwarted with appropriate levels of physical protection and can be easily detected in wired media through impedance mismatching), in the wireless media signals propagate in all directions, allowing any potential adversary to eavesdrop without revealing their presence. This is disconcerting as it means that the weaknesses inherent in securing wireless networks start at the lowest layer and, unfortunately, the tradition has been to apply *only* higher-layer cryptographic protocols to securing wireless networks. The past couple of years, however, have seen an explosion of efforts to tap into the physical layer[1] as a source for new forms of security. Generally, using the lower-layers for security involves one of a few different strategies: disseminating secret information through the channel so that legitimate parties are able to share information in spite of an eavesdropper "tapping" into the channel; exploiting the physical layer as a source of unique information to distinguish between transmitters; exploiting the shared randomness in radio communications, as it exemplified by the underlying fading process in a mobile environment, to support key establishment; and using the physical layer appropriately to ensure the availability of core communication services. We have selected four papers that represent these four directions and ultimately provide evidence that the lower layers of the wireless protocol stack can, in fact, be used to support the security objectives of confidentiality, authentication, and availability.

Another key feature that distinguishes wireless communications from other types of communication networks is the rapidity at which new *emerging* wireless technologies arrive on the scene. In just the past few years there has been an explosion of interest in sensor networks, vehicular networks, cognitive radio networks, and RFID networks. As an editorial team, we were very interested in representing these new technologies and highlighting the security challenges that they will face, as well as the unique solutions that must be brought to bare on them in order to ensure that these emerging networks have levels of security comparable to what one would find in more "static and less evolving" types of networks. Unfortunately, we were not able to find any papers on cognitive radio network security or RFID security that met our selection criteria. However, we found that the contributors had identified several exciting problems in vehicular ad hoc networks (VANETs) and sensor networks. Hence, our second section, which focuses on security and privacy for emerging wireless networks, includes four papers: two addressing security issues for VANETs and two addressing security issues for sensor networks. Examining these four papers, the reader might notice a few *emerging* themes: energy efficiency is an important concern for wireless networks, and wireless networks inherently introduce opportunities for breaching privacy.

The last section of our special issue is devoted to securing wide area wireless networks. The success of wireless technologies, admittedly, started from the ability for cellular communications to provide affordable, wide area connectivity to a large consumer base. Even though wireless technologies have tended to become "more local", as evidenced by the emergence of technologies like RFID and sensor network systems, it is undeniable that broadband, wide area communications represents an exciting future for the communications industry. Recently, there has been a surge in activity in the standards communities to ratify wide area wireless technologies. Perhaps the most notable of these technologies is 802.16 or simply WiMax. The various 802.16 standards were written to support different forms of network access, ranging from static to mobile. Consequently, there will be many forms

[1] The editors shamelessly acknowledge that the pun here was intentional.

of accessing WiMax networks and hence many attack modalities that an adversary can employ against WiMax networks. We have chosen three papers to comprise our last section and round out this special issue. As the reader peruses these papers, we would again draw their attention to some recurring underlying themes: efficiency is important in designing security mechanisms for wireless networks, and one should be very concerned about the ease with which communications can be listened to and tracked. Returning to the papers of this section, two of the three papers are focused on specific security issues arising in WiMax/802.16 networks. The third paper, however, might seem to be a little out of place amidst two papers targeted at wide area networks. As an editorial team, we felt that the last paper of this section (and of the entire special issue) should return the reader's focus to the fundamentals behind designing a secure network. Hence, in our viewpoint, the last paper presents a formal treatment of security issues for wireless networks like WiMax networks, and also serves to tie all of the papers together in this special issue.

Overall, we believe that this special issue on wireless security will provide an important contribution to the community as wireless networks continue to emerge and face a constantly evolving array of threats. As an editorial team, we would note the importance of wireless technologies as the primary form of communication that we use access to each other and the broader Internet, and hence we encourage researchers to continue exploring the security problems that arise across the heterogeneity of wireless technologies.

Adrian Perrig is a Professor in Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science at Carnegie Mellon University. Adrian serves as the technical director for Carnegie Mellon's Cybersecurity Laboratory (CyLab). He earned his Ph.D. degree in Computer Science from Carnegie Mellon University, and spent three years during his Ph.D. degree at the University of California at Berkeley. He received his B.Sc. degree in Computer Engineering from the Swiss Federal Institute of Technology in Lausanne (EPFL). Adrian's research revolves around building secure systems and includes network security, trustworthy computing and security for social networks. More specifically, he is interested in trust establishment, trustworthy code execution in the presence of malware, and how to design secure next-generation networks. More information about his research is available on http://www.ece.cmu.edu/~adrian Adrian's web page. He is a recipient of the NSF CAREER award in 2004, IBM faculty fellowships in 2004 and 2005, and the Sloan research fellowship in 2006.

Wade Trappe received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently Associate Director at the Wireless Information Network Laboratory (WINLAB) and an associate professor in the Electrical and Computer Engineering Department at Rutgers University. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, has developed jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers, including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers in premier conferences. His experience in network security and wireless systems spans 12 years, and he has co-authored a popular textbook in the field, Introduction to Cryptography with Coding Theory, as well as four other books on wireless systems and multimedia security. He is a member of the IEEE Signal Processing and Communications societies, and a member of the ACM.

Virgil Gligor received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. Prior to joining Carnegie Mellon, Gligor was at the University of Maryland from 1976, and was a Professor of Electrical and Computer Engineering. Over the past 29 years, his research interests have ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. He was a consultant to the Burroughs (1977-1981) and IBM (1984-1999) Corporations, and is currently serving on Microsoft's Trusted Computing Academic Advisory Board. He served the profession as the chair or co-chair of several conferences and symposia, including the IEEE Security and Privacy Symposium, the Internet Society's Network and Distributed Systems Security Symposium, the IEEE Dependable Computing for Critical Applications, and the IEEE-ACM Symposium on Relaibility in Distributed Software and Databases. He received the outstanding paper award at the 1988 IEEE Symposium on Security and Privacy. He was a member of several U.S. Government INFOSEC Study Groups that set research agendas in information security, and served on a National Research Council panel on information security.

Radha Poovendran is an Associate Professor and founding director of the Network Security Lab (NSL) at the Electrical Engineering Department of the University of Washington. He received his Ph.D. in Electrical Engineering from the University of Maryland, College Park in 1999. His research interests are in the areas of applied cryptography for multiuser environment, wireless networking, and applications of Information Theory to security. He is a recipient of the NSA LUCITE Rising Star Award and Faculty Early Career Awards including NSF CAREER (2001), ARO YIP (2002), ONR YIP (2004), and PECASE (2005) for his research contributions to multiuser security and the Graduate Mentor Recognition Award from the University of California San Diego in 2006. He has recently organized and co-chaired the 2008 National Workshop on High Confidence Transportation Cyber-Physical Systems (CPS) and chaired the 2009 Army Research Office Workshop on CPS security at University of Washington. He is a co-editor of the Springer Verlag book "Secure localization and time synchronization in wireless ad hoc and sensor networks," and guest editor of an upcoming special issue on Cyber- Physical Systems in the Proceedings of the IEEE.

Heejo Lee is an associate professor at the Division of Computer and Communication Engineering, Korea University, Seoul, Korea. Before joining Korea University, he was at AhnLab, Inc. as a CTO from 2001 to 2003. From 2000 to 2001, he was a postdoctorate at the Department of Computer Sciences and the security center CERIAS, Purdue University. Dr. Lee received his B.S., M.S., Ph.D. degree in Computer Science and Engineering from POSTECH, Pohang, Korea. Dr. Lee serves as an editor of the Journal of Communications and Networks. He has been an advisory member of Korea Information Security Agency and Korea Supreme Prosecutor's Office. With the support of Korean government, he worked on constructing the National CERT in the Philippines (2006) and consultation on cyber security in Uzbekistan (2007) and Vietnam (2009). More information is available at http://ccs.korea.ac.kr.