2010

Security in next generation wireless networks

Wanlei Zhou

Haining Wang
William & Mary, hnw@cs.wm.edu

Recommended Citation

Xiang, Y., Zhou, W., & Wang, H. (2010). Security in next generation wireless networks. Security and Communication Networks, 3(1), 1-3.

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2010; **3**:1–3
Published online 25 September 2009 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.151

Guest Editorial

Security in next generation wireless networks

By Dr Yang Xiang, Prof. Wanlei Zhou, and Dr Haining Wang

In the past decades, the evolution of wireless technologies has brought significant changes in modern communication networks through its wireless extension of wired networks. Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. However, risks are inherent in any wireless network. As the technologies of next generation wireless networks are emerging, security has become a primary concern in order to provide dependable and secure communication between the wireless nodes in a hostile environment. The next generation wireless networks face many unique challenges in security such as open network architecture, shared wireless medium, limited resource constraints, and highly dynamic network topology. This special issue in Security and Communication Networks presents current research focusing on the standard or protocol related security, attacks and defense applications, security architecture and frameworks, and theories and methodologies in security in next generation wireless networks.

In view of this, we selected eight papers on security in next generation wireless networks to this special issue. The papers are either selected from open submissions or the best paper in 2008 International Workshop on Network and System Security (NSS 2008), held on 18–19 October 2008, in Shanghai, China. All the papers were selected on the basis of their originality, technical quality, and significance. Each paper was under rigorous technical review by at least three international reviewers. The selected papers are summarized below.

Routing security contexts *via* an IP network imposes new challenging requirements of secure cross-handover services and security context management. In the first paper, Kim and Shin present a context router that manages security contexts in an all-IP network, providing seamless and secure handover services for the mobile users that carry multimedia-access devices. The proposed predictive routing mechanism improves seamless and secure cross-handover services.

Trust establishment and management are essential for any security framework of MANETs. In the second paper, Dahshan and Irvine propose a robust self-organized, public key management for MANETs. The proposed scheme relies on establishing a small number of trust relations between neighboring nodes during the network initialization phase. Simulation results show that the proposed scheme is robust and efficient in the mobility environment of MANET and against malicious node attacks.

A mobile node in a MANET must be assigned a free IP address before it may participate in unicast communications. This is a fundamental and difficult problem in the practical application of any MANET. In the third paper, Zhou, Mutka, and Ni propose a secure autoconfiguration algorithm, namely secure prophet address allocation, to perform prophet address allocation while considering the requirements of communication overhead, latency, and scalability. It is demonstrated that the proposed approach is able to maintain uniqueness of address assignment in the presence of IP spoofing attacks, 'state pollution' attacks, and Sybil attacks.

In the fourth paper, Babu and Venkataram present a security techniques selection scheme for mobile transactions, called the Transactions-Based Security Scheme (TBSS). The TBSS identifies a suitable level

of security techniques from the repository, which consists of symmetric, and asymmetric types of security algorithms arranged in three complexity levels, covering various encryption/decryption techniques, digital signature schemes, and hashing techniques. Their results shows a considerable reduction in security cost compared to static schemes, which employ pre-fixed security techniques to secure the transactions data.

Discriminating impersonating devices is an important problem in Wi-Fi networks. While legal and illegal nodes may have the same configuration, their locations are different, resulting in different RSSI measured by the sensors. In the fifth paper, Tao *et al*. proposed X-mode, a faster clustering algorithm, to process the data. X-mode differs from other clustering algorithms by dropping low RSSI values and treating data points with the same RSSI values as one point during computation.

Many RFID authentication techniques require a form of synchronization between a tag and a reader. A de-synchronization could jeopardize security and privacy. In the sixth paper, Conti *et al*. proposed a hash-chain based scheme to resolve the de-synchronization problem in RFID systems. Their solution achieves mutual reader-tag authentication by utilizing hash traversal and Merkle tree techniques. Through extensive simulations, the authors show that the tag and the reader can easily recover from de-synchronization with negligible overhead.

Improving wireless access security through various OSI PHY layer mechanisms is the focus of the seventh paper. Klein *et al*. investigated the exploitation of RF waveform features that are inherently unique to specific devices and could be use for reliable device classification. They introduce a Dual-Tree Complex Wavelet Transform (DT-CWT) denoising technique to augment and improve Variance Trajectory (VT) detection capability. Instantaneous amplitude responses from collected 802.11a signals are used to validate the efficacy of DT-CWT at varying SNR.

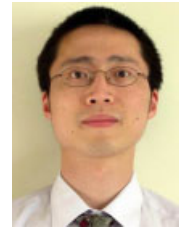
Internet key exchange version 2(IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. In the eighth paper, Faigl *et al*. evaluated the performance impacts of IKEv2 in the next-generation wireless networks. They conduct experiments on two different wireless authentication methods, pre-shared keys (PSK) and extensible authentication protocol (EAP). Their experimental results clearly demonstrate the practical costs involved for IKEv2 authentication.

We sincerely hope that you will enjoy reading these eight papers and find them very useful. We thank all the international reviewers for their professional services. We deeply thank Professor Hsiao-Hwa Chen, the Editor-in-Chief, for providing this opportunity to publish this special issue. Without his continuous support, encouragement, and guidance throughout this publishing project, the success of this special issue is impossible.

Hahnsang Kim and Kang Shin, On predictive routing of security contexts in an All-IP network.
Hisham Dahshan and James Irvine, A robust self-organized public key management for mobile *ad hoc* networks.
Hongbo Zhou, Matt W. Mutka, and Lionel M. Ni, Secure prophet address allocation for MANETs.
Sathish Babu B. and Pallapa Venkataram, Random security scheme selection for mobile transactions.
Tao *et al*., A data clustering approach to discriminating impersonating devices in Wi-Fi networks.
Conti *et al*., eRIPP-FS: a novel authentication technique for RFID.
Klein *et al*., Application of wavelet denoising to improve OFDM-based signal detection and classification.
Faigl *et al*., Performance evaluation of IKEv2 authentication methods in next generation wireless networks.

Dr Yang Xiang
Central Queensland University, Australia
Prof. Wanlei Zhou,
Deakin University, Australia
Dr Haining Wang
College of William and Mary, U.S.A.

Authors' Biographies



Yang Xiang is currently with School of Management and Information Systems, Central Queensland University. His research interests include network security and distributed systems. In particular, he is currently working in a research group developing active defence systems against large-scale network attacks and new Internet security countermeasures. He has served as PC Chair for the 11th IEEE International Conference on High Performance Computing and Communications (HPCC 2009), the 3rd International

DOI:10.1002/sec

Conference on Network and System Security (NSS 2009), and the 14th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2008). He has been PC member for many international conferences such as IEEE ICC, IEEE GLOBECOM, and IEEE ICPADS. He is on the editorial board of Journal of Network and Computer Applications.

Wanlei Zhou received his Ph.D. degree from The Australian National University, Canberra, Australia, in October 1991. He also received the D.Sc. degree from Deakin University, Victoria, Australia in 2002. He is currently the Chair Professor of Information Technology and the Associate Dean (International), Faculty of Science and Technol-ogy, Deakin University, Melbourne, Australia. His research interests include distributed and parallel systems, network security, mobile computing, bioinformatics, and e-learning. Professor Zhou has pub-lished more than 170 papers in refereed international journals and refereed international conferences proceedings. Since 1997, he has been involved in more than 50 international conferences as General Chair, Steering Chair, PC Chair, Session Chair, Publication Chair, and PC member. Professor Zhou is a Senior member of the IEEE.

Haining Wang is an Associate Professor of Computer Science at the College of William and Mary, Williamsburg, VA. He received his Ph.D. in Computer Science and Engineering from the University of Michigan at Ann Arbor in 2003. His research interests lie in the area of networking, security, and distributed computing. He is particularly interested in network security and network QoS (Quality of Service) to support secure and service differentiated internetworking.

DOI:10.1002/sec