Mobile Netw Appl (2013) 18:664–665
DOI 10.1007/s11036-013-0471-x

Editorial for Security and Privacy in Wireless Networks Special Issue

Muttukrishnan Rajarajan · Steven Furnell

Published online: 13 October 2013

Editorial:

This special issue features five invited papers from experts working in the area of wireless security and privacy. The first article, "Trust-based routing mechanism in MANET: Design and Implementation", discusses the challenging issues in MANET routing security. The authors present FrAODV, a trust-based scheme for securing AODV routing protocol in MANET using the friendship mechanism. In their proposed scheme the nodes can evaluate the routing paths according to some selected features (such as node reputation and identity information) before forwarding the data through these routes. They have used two types of implementation in their scheme, simulation (using NS-2) and a real test-bed (using JADHOC). The proposed scheme is believed to provide a robust environment where MANET nodes can trust each other in a secure community.

The second article, entitled "Performance of IEEE 802.11 under Jamming", studies the performance of the IEEE 802.11 MAC protocol under a range of jammers that covers both channel-oblivious and channel-aware jamming. The authors consider two channel-oblivious jammers: a *periodic* jammer that jams deterministically at a specified rate, and a *memoryless* jammer whose interfering signals arrive according to a Poisson process. They also develop new models for channel-aware jamming, including a *reactive* jammer that only jams non-colliding transmissions and an *omniscient* jammer that optimally adjusts its strategy according to current states of the participating nodes. The study comprises of a theoretical analysis of the saturation throughput of 802.11 under jamming, an extensive simulation study, and a testbed to conduct real world experimentation of jamming IEEE 802.11 using software defined radio (GNU Radio combined with USRP boards).

In the third paper, "Adaptive Information Coding for Secure and Reliable Wireless Telesurgery", a Telesurgical Robot System (TRS) is studied and the authors present a novel approach that uses information coding to integrate both light-weight privacy and adaptive reliability in a single protocol called Secure and Statistically Reliable UDP (SSR-UDP). They prove that the offered security is equivalent to the existing AES-based long key crypto systems, yet with significantly less computational overhead. They also demonstrate that the proposed scheme can meet high reliability and delay requirements of TRS applications in highly lossy environments while optimizing the bandwidth use.

The fourth paper is entitled "Reverse authentication in financial transactions and identity management", and the authors utilise the concept that new families of protocol, based on communication over human-based side channels, can permit secure pairing or group formation in ways such that no party has to prove its name. In this model, individuals are able to hook up devices in their possession to others that they can identify by context. They examine a model in which, to prove his or her identity to a party, the user uses one of these human-interactive security protocols (or HISPs) to connect to it. Thus, when authenticating A to B, A authenticates a channel she has to B: the reverse direction. This can be characterised as bootstrapping a secure connection using human trust. This provides new challenges to the formal modelling of trust and authentication.

In the fifth paper, titled "A privacy preserving method using privacy enhancing techniques for location based services", the authors study the privacy issues relating to gathering of location information for non-trusted applications like location-based marketing or user behaviour profiling. It shows how

M. Rajarajan (✉)
Security Engineering, City University London, Northampton Square, EC1V 0HB London, UK
e-mail: R.Muttukrishnan@city.ac.uk

M. Rajarajan
e-mail: rajarajan.city@gmail.com

S. Furnell
Centre for Security, Communications & Network Research, Plymouth University, Drake Circus, PL4 8AA Plymouth, UK
e-mail: S.Furnell@plymouth.ac.uk

users can limit their location information provided to a service, but these controls are simple, making it important for the user to understand how their location information is being used by services. This paper reviews some of the methods currently being proposed to reduce the impact of location tracking on user privacy, and presents a novel encryption method for preserving the location and trajectory path of a user using Privacy-Enhancing Technologies.

In the sixth paper titled "Ubiquitous One-Time Password Service using the Generic Authentication Architecture (GAA)" the authors show how Trusted Computing can be extended in a GAA-like framework to offer new security services. They propose a general scheme that converts a simple static password authentication mechanism into a one-time password (OTP) system using the GAA key establishment service. The proposed scheme employs a GAA-enabled user device and a GAA-aware server. Most importantly, unlike most OTP systems using a dedicated key-bearing token, the user device does not need to be user or server specific, and can be used in the protocol with no registration or configuration.

The guest editors are thankful to our reviewers for their effort in reviewing the manuscripts.

Muttukrishnan Rajarajan is a Professor of Security Engineering at City University London where he leads the Information Security research activities. He has research expertise in the areas of privacy preserving techniques, mobile security and Cloud security. He acts as an advisor to the government of India research laboratories in the area of cyber security. He is a visiting scientist at the British Telecommunications (BT) security innovation laboratories, UK. Professor Rajarajan is a Senior Member of Institute of Electrical and Electronic Engineering and is a member of the academic advisory board of the institute of information security professionals (IISP). He has been involved in several recent policy debates in the area of cyber security. He has published more than 200 journal and conference papers and has recently published a book entitled *Mobile Security and Privacy.* He is in the advisory board of several start-up companies in the area of Cloud security and Identity assurance. He serves on several journal editorial boards and international conferences technical programme committees. More details can be found at www.staff.city.ac.uk/~raj.

Prof. Steven Furnell is the head of the Centre for Security, Communications & Network Research at Plymouth University in the United Kingdom, and an Adjunct Professor with Edith Cowan University in Western Australia. His interests include security management and culture, computer crime, user authentication, and security usability. Prof. Furnell is active within three working groups of the International Federation for Information Processing (IFIP) - namely Information Security Management, Information Security Education, and Human Aspects of Information Security & Assurance. He is the author of over 240 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalizing the Information Society (2001) and Computer Insecurity: Risking the System (2005). He is also the editor-in-chief of Information Management & Computer Security, and the co-chair of the Human Aspects of Information Security & Assurance (HAISA) symposium (www.haisa.org). Steve is active in a variety of professional bodies, and is a Fellow of the BCS, a Senior Member of the IEEE, and a full member of the Institute of Information Security Professionals. Further details can be found at www.plymouth.ac.uk/cscan, with a variety of security podcasts also available via www.cscan.org/podcasts. Steve can also be followed on Twitter (@smfurnell).