Introduction

Ashley Podhradsky

Dakota State University,
820 N Washington Ave.,
Madison, SD 57042, USA
E-mail: Ashley.podhradsky@dsu.edu

Biographical notes: Ashley Podhradsky is an Assistant Professor within the Computer and Network Security Programme at Dakota State University in Madison, South Dakota. Her current research focuses on developing digital forensics standards for non-traditional devices, specifically the Xbox 360. With more communication moving from traditional computing devices to non-traditional devices such as gaming systems, there is a strong need for forensic experts who can analyse these systems. Her work has been published in several journals, conference proceedings, and she serves as an expert contributor to the media community. She received an Anita Borg Scholarship for Women in Computing which was sponsored by Google in 2007. She received a WISE Summer Research Fellowship from the TRUST Organization during 2011 and 2012. She is an active member of the InfraGard and the High Technology Crime Investigation Association.

Given the explosion of mobile networks, it is more prudent than ever to ensure the security of mobile networks and transmitted confidential data. As businesses, governments, and individuals move towards mobile devices and applications for conducting private transactions, the data in transit and the data at rest needs to be secure from interception and unauthorised access. Mobile networks encompass much more than just traditional desktop and notebook computers. Mobile networks include smart phones, tablets, TV's, entertainment devices such as gaming consoles, in addition to traditional desktop and notebook computers. This special issue features articles focused on the security and privacy in different mobile environments, privacy guidelines, privacy frameworks, smart phone privacy, gaming console network security, and energy-efficient data aggregation for wireless sensor networks. The goal of this special issue of the *IJMNDI* edition is to provide a respected source for research dissemination for our contributors, and a source of cutting edge, high quality information within the field of security for mobile networks for our readers.

In the article 'Privacy disclosure risk: smartphone user guide', the authors introduce an online survey to understand the perception of privacy practices among users. In addition, the authors provide a guideline to mitigate privacy risk incidents on smartphones. The mobile platform of a popular gaming console is researched in 'An analysis of security vulnerabilities of the Xbox 360 and Xbox Live mobile network'. As gaming consoles migrate from single player embedded environment with rudimentary communication capabilities to networked devices capable of all the communication seen in modern computers, securing the devices have never been more important. This paper introduces a survey and study aimed at determining the perceived security of the devices, in addition to the actual security vulnerabilities. In 'Agent-based modelling to visualise trustworthiness: a socio-technical framework', the Florida State University authors introduce a socio-technical research focused on deceptive behaviours in virtual collaborative environments that are based on physical world scenarios. The goal of the work is to develop modelling strategies to gauge the trustworthiness of an agent based on systematically captured data. In order to monitor wireless mobile regions, detect events, and acquire transmission data, the authors of 'Secure and energy-efficient data aggregation for wireless sensor networks' introduce two energy-efficient data aggregation schemes. The schemes aim to detect malicious nodes, and ensure no forged aggregation results are accepted by the base station.