



Security, Trust and Privacy in Online Systems: Introduction to Special Edition

Steven Furnell*

*Centre for Security, Communications & Network Research, University of Plymouth

Introduction

This special issue presents four papers focusing upon the interrelated issues of security, trust and privacy in online systems; which can collectively be regarded as essential underpinnings if we are to maximise the opportunities offered by networked information technologies. However, past experience demonstrates that their fundamental importance does not guarantee that they will be addressed correctly or given sufficient consideration by the participants in online systems. Specific attention is therefore required in order to ensure that security is approached in a methodical and informed manner, rather than selected, designed and implemented on an ad hoc basis. To do this often requires innovative approaches, and although security is an established domain the papers in this issue demonstrate that there is still significant scope for further advancing the understanding and associated practice.

The first paper, by Nance et al. considers the issue of providing security training, looking at the considerations and stages involved in establishing a virtualised laboratory environment. The authors recognise that security education can itself represent a challenging prospect, with a requirement to address the provision of hands-on, practical skills within what is an implicitly sensitive topic area. The use of virtualization technologies is considered to provide a viable and economic solution, enabling entire networks to be run within a single physical machine. In a practical sense, the virtual systems function exactly as they would if running on physical hardware, while at the same time permitting a variety of security configurations to be assessed without introducing any risk to production network environments. The paper reviews three real-life examples of such laboratories, examining the methodologies followed in each case and the related principles that others might follow in achieving their own implementations.

The paper from Williams presents work situated in the explicitly sensitive domain of healthcare, where the potential for shared electronic patient information can represent a significant consideration for the security of medical data. Through an examination in the specific context of primary care, it is recognised that staff frequently rely upon trust assumptions, on the basis that they do not fully understand the threats to which

Corresponding author: S. Furnell, Centre for Security, Communications & Network Research, University of Plymouth, Plymouth, UK PL4 8AA. Tel.: +44(0)1752 586234. E-mail: s.furnell@plymouth.ac.uk

systems and data are exposed, or the security concepts that are intended to protect them. In this context, it is essential to understand how trust aspects interrelate with consequent security practices. To this end, the author's approach investigates trust and its influences on practice through a novel triangulation of interviews, observation and physical artefacts. This enables exposure of the underlying trust culture of the staff, identifying their related behaviours and how these serve to inform their decisions and actions.

The next paper, from Katos, considers a model for online transactions; the data exchanges that can occur between a consumer and a supplier in an Internet context. From a review of existing theoretical perspectives, the author proposes a framework for understanding how a series of initial predicting factors and mediating mechanisms can ultimately influence online transactions. These predicting factors refer to the key reasons that may initially make consumers hesitant in online transaction contexts, and may include trust beliefs, perceived usefulness and ease of use. The author's model aims to explain the mediating mechanisms that can take place between this stage and the end point of the resulting transaction. By exposing this so-called 'black box' aspect, the model is able to take account of user behavioural factors (e.g. their security and privacy concerns, risk perceptions and willingness to provide information) in determining the impact/outcome of the transaction. Thus it provides new insights and understanding of the overall transaction process that occurs in online contexts.

The final paper, by Phippen et al. consider the challenges posed by the relatively new phenomenon of social networks, which have finally begun to provide a large-scale means for users to create online content rather than just consume it from other sources. Unfortunately, the exact nature of *what* people choose to post about themselves can often pose tremendous risks to their own data, inviting problems such as identity theft and unanticipated invasion of privacy. Additionally, the more relaxed attitudes that some people tend to exhibit online can lead to a greater willingness to establish relationships and share data than they would normally entertain in the physical world. Phippen et al. look at the nature of personal data to be found on social networking pages, determining that much of it is sensitive and unprotected. From this basis, they proceed to conduct research into users' readiness to approach strangers to become their online friends, based upon the social engineering-style lures of enticing profile photographs and public profiles (the notable point being that by establishing the friendships, the strangers are then allowed access to the personal details that the users themselves have published on their own pages).

The papers collectively demonstrate the importance of approaching security and related issues in a structured manner, with each also making an individual contribution that advances the thinking and practice for doing so. Moreover, each of them demonstrate advancement of the associated approaches for approaching and realising security, offering innovative perspectives and solutions that would not have been realised through traditional methods.