JISSec 8(2) 2012

Journal of
Information System
Security

www.jissec.org

Editorial

In search of what Information Security might be

Ever since the topic area of information security became popular, there has been significant confusion as to what information security might be. I was recently at a seminar where the presenter kept discussing how personality profiles should be studied and how such a study would help in training individuals to comply with cyber security policies. This was an excellent piece of work, albeit in the area of defining personality profiles. I have always felt that as research into any domain progresses we often lose sight of the artifact in question. In the context of information security research, the question is – should we be focusing attention on personality profiles as a topic area for our research (or something similar), or should we be focusing on aspects of compliance, or should we make the artifact of security policies central to our argument. This does not mean that research looking into the sociological, physiological or economic aspects of information security should be ignored or not published. It is important however to define what constitutes research **in** information security as opposed research **about** information security. Majority of the "new" breed of research seems to be peripheral to the artifact and falls in the later category.

The problem of researching the core artifact is not just germane to information security researchers. A similar pattern was identified amongst management information systems scholars. In a June 2003 editorial in *MIS Quarterly* Ron Weber notes information systems researchers desperation in "seeking the IT artifact". There was also an earlier commentary published on the same topic area in *Information Systems Research* by Wanda Orlikowski in June 2001. The question that begs attention is – what is the core of information security research?

One definition of a security artifact is that it is a protocol, a device, architecture, an entire system or an application environment. While this definition of an artifact is fairly generic, in our context it may be worthwhile thinking about security artifacts in terms of three models – representational model, decomposition model and the state-tracking model (see {Thomas, 2012 #2019}). The representational model is *surface structural* at best, *i.e.* it represents security in terms of a triple – the security rules, what they mean and how the rules represent the meaning. The decomposition model describes the structural and behavioral properties associated with security and is *deep structural* in nature. The state-tacking model transcends the *surface* and *deep structures* and is composed of how security is mapped, tracked, reported and sequenced. I believe that the security artifact has to be integral to the *surface* and *deep* structures of security. In cases where it is not, the research is perhaps a little too detached from the core.

I don’t think these questions can be addressed in a single issue of a journal. However I do believe that it will open up an opportunity to engage in a public discourse. To that effect we are going to publish a series of papers exploring what information security might be. The first of such papers appears in this issue of the journal. Comments and suggestions on the topic area are re welcome as are letters to the editor and/or authors.

In order to set the tone exploring what information security might be, the first paper of this issue presents an Understanding of Information Security”. Authored by Romilla Chowdhuri and Gurpreet Dhillon of Virginia Commonwealth University, USA the paper explores the mystical nature of information and security. The paper takes a reader through the definition of information, systems and security. A socio-philosophical analysis helps in understanding the ontological and epistemological aspects of the concept.

The second paper is “Managing Corporate Computer Crime and the Insider Threat: the Role of Cognitive Distortion Theory” by Mark A. Harris, University of South Carolina (USA). This paper investigates integrity of individuals through the perspective of Cognitive Distortion Theory. Cognitive distortions are conceptualized as thoughts used to minimize, justify, or rationalize inappropriate behaviors, such as lying and stealing. The paper reports an interesting finding that even though a cognitive distortion oriented training may be imparted to individuals there is no significant impact on the “how I think” scores, one of the primary ways for defining cognitive distortion.

The third paper is “Online identity theft: a longitudinal study of individual threat-response and coping behaviors” by Murugan Anandarajan, Narasimha Paravastu, Bay Arinze, Rob D’Ovidio. The authors presents findings based on an Extended Parallel Process Model to test adequacy of the model to predict individual intention to engage in behaviors that reduce risks of identity theft. The findings suggest that when users are fully aware of the threats, they are in a better position to cope with the problem. One of the main contributions of the study is the impact fear appeals have on perception of threats.

I hope that you enjoy this issue and I look forward to have an engaging discourse on the nature and scope of information security, particularly with respect to the relevance of current research directions and how the security artifact is considered in research.

References

Thomas, M. and G. Dhillon (2012). "Interpreting Deep Structures of Information Systems Security." The Computer Journal **55**(10): 1148-1156.