doi:10.1093/comjnl/bxs137

Capsule Reviews

Fairouz Kamareddine

The Capsule Reviews are intended to provide a short succinct review of each paper in the issue in order to bring it to a wider readership. The Capsule Reviews were compiled by Fairouz Kamareddine. Professor Kamareddine is an Associate Editor of *The Computer Journal* and is based in the Department of Mathematical and Computer Sciences at Heriot-Watt University, Edinburgh, UK.

Interpreting Deep Structures of Information Systems Security. Manoj Thomas and Gurpreet Dhillon

In terms of information systems (ISs) security, surface structures refer to the obvious security mechanisms (locks, keys, passwords and firewalls), while deep structures refer to the manner in which the passwords and firewalls make sense in a given context. This paper considers the deep and surface structures of IS security in terms of three models: the representational (surface structure level) model, the state-tracking (interface of surface and deep structures) model and the decomposition model (deep structure level). The authors argue that lack of integrity between these three models leads to significant security concerns. After a review of the state of affairs in IS security, the authors conclude the need to define models that can be used to describe the ontological constructs and the grammar that manifest real-world IS security system. Then, the authors propose the deep structures of IS security models, which include the representational model, the state-tracking model and the decomposition model. The state-tracking model interfaces with the representational and decomposition models to maintain integrity. To demonstrate the nature of the model, the authors look at a series of real events that lead to a security incident at a university computing center and show that combining features from the three models can manifest in the agility and flexibility needed in a real-world information security model to ensure confidentially, integrity and availability.

A Provably Secure Construction of Certificate-Based Encryption from Certificateless Encryption. Wei Wu, Yi Mu, Willy Susilo, Xinyi Huang and Li Xu

Although certificates can solve the public-key authenticity problem, it requires an addition burden to manage the certificates among the whole system, which are costly to use in practice. Al-Riyami and Paterson introduced the notion of certificateless public-key cryptography which does not require public-key certificates. Owing to the lack of certificates, malicious parties can replace an entity's public key with a false key, and other entities may be duped to use the false key in encryption and signature verification. Certificate-based encryption (CBE) has been proposed, which ensures the authenticity of the public key and is used for decryption. Although CBE has public-key certificates, it works in a similar way to certificateless encryption (CLE). This paper provides a provably secure approach to convert CLE schemes into CBE schemes. After an introduction to CBE and CLE, the potential adversaries on CBE (normal, strong and super) are defined and security against various adversaries is given. It is then shown how to convert a CLE scheme into a CBE scheme. The correctness of the proposed scheme CLE-2-CBE is ensured by the underlying CLE. To demonstrate the application of the generic construction, a concrete CBE scheme from a CLE scheme is described.

Casting Ballots over Internet Connection Against Bribery and Coercion. Yufang Chung and Zhen-Yu Wu

Uncoercibility means that voters can vote of their own free volition even under conditions of bribery and coercion. The aim of this paper is to design an e-voting scheme that can totally guard against bribery and coercion to achieve uncoercibility. The proposed password-based scheme is composed of three phases: authentication phase, voting phase and announcing phase. After a brief introduction to the needed preliminaries, the three phases of the scheme are given and it is shown that this proposed password-based e-voting scheme can satisfy all security requirements of electronic election, including anonymity, eligibility, fairness, mobility, uniqueness, verifiability and uncoercibility. A comparison of the scheme with six other existing schemes from the literature is given.