Journal of Universal Computer Science, vol. 19, no. 16 (2013), 2347-2348
submitted: 18/9/13, accepted: 29/9/13, appeared: 1/10/13 © J.UCS

Information Security

J.UCS Special Issue

Ilsun You
(Korean Bible University, Seoul, Republic of Korea
ilsunu@gmail.com)

Edgar Weippl
(Vienna University of Technology, Austria
and
SBA Research, Vienna, Austria
weippl@ifs.tuwien.ac.at)

We are proud to present this special issue of the Journal of Universal Computer Science, which contains a selection of papers from the 2013 Asian Conference on Availability, Reliability and Security (AsiaARES 2013), which was held in Gadjah Mada University, Indonesia on 25-29 March, 2013. The contributions selected are a good representation of the wide range of privacy and security-related topics discussed at the conference.

The papers reflect challenges that have arisen with new technologies and new modes of communication and data use, from cloud computing and mobile phones to social network services, such as Twitter. Once again, this demonstrates that the papers presented at AsiaARES 2013 are not only of academic interest but have their fingers on the pulse of the user.

Xingxing Xie et al. propose a solution to the issue of secure attribute and user revocation in the use of attribute-based encryption in cloud computing. Their ciphertext-policy attribute-based access control construction minimizes the computation overhead for data service managers and data owners by allowing the efficient enforcement of authorization policies, including attribute and user revocation.

In their paper "Multiplication and Squaring with Shifting Primes on OpenRISC Processors with Hardware Multiplier", Leandro Marin et al. present an optimization of elliptic curve cryptography using shifting primes. Their method is potentially applicable in scenarios where the security interoperability between class-1 and class-2 constrained devices is required, e.g. in the future Internet of Things.

Youngho Park et al. propose a secure message delivery protocol for protecting the privacy of the receiver's location in social spot-based Vehicular Delay Tolerant Networks. In their protocol, they replace conventional pseudonym-based vehicle identification with identity-hidden message indexing and a non-interactive key agreement scheme to establish a secure communication channel that allows the recipient to remain anonymous. This reduces cryptographic overhead while providing efficient privacy preservation.

Tran Phuc Ho et al. utilize a graph-based KNN algorithm to detect spam SMS - both advertising and malicious text messages - on mobile devices and smartphones. An evaluation using two SMS different corpora showed that the algorithm identifies text messages with high accuracy, and that the processing time is short enough to detect spam in real time.

Bo Liu et al. present an extended real-time privacy amplification (RTPA) scheme with an authentication procedure based on the CLIP system, thus utilizing quantum key distribution technology. The RTPA scheme requires authentication to prevent man-in-the-middle attacks. Their proposed solution converts weak secret strings into unconditionally secure keys.

Another paper that addresses mobile phone communications is "Security Issues and Attacks on the GSM Standard: a Review" by Giuseppe Cattaneo et al. The authors discuss vulnerabilities and attacks on the GSM protocol, in particular impersonation attacks focusing on the A5/1 algorithm, which protects over-the-air communication and is still used as a fallback option in GSM networks despite being mostly replaced by newer algorithms. The paper reviews possible solutions – both from academia and informal sources – and discusses their feasibility.

Ting Cui and Chenhui Jin focus on impossible differential cryptanalysis and show how to retrieve longer (m^2+1 or m^2+2 rounds) impossible differentials for m-cell Skipjack_{SP} and Skipjack_{SPS}. This is done by configuring the P layer as a binary matrix.

The final paper in this issue, "Text Analysis for Monitoring Personal Information Leakage on Twitter" by Dongjin Choi et al. proposes a coefficient method for identifying unintentionally exposed personal information on social networking services. Their analysis shows that this method has better results than a standard word matching method.

We hope that you find the contributions in this special issue and the different aspects of availability, reliability and security they address interesting.

Ilsun You
Edgar Weippl
Guest Editors