2014

Security of new generation computing systems

Xu Li
Fujian Normal University, xuli@fjnu.edu.cn

Elisa Bertino
Purdue University, bertino@cs.purdue.edu

Yi Mu
University of Wollongong

Follow this and additional works at: http://docs.lib.purdue.edu/ccpubs
Part of the Engineering Commons, Life Sciences Commons, Medicine and Health Sciences Commons, and the Physical Sciences and Mathematics Commons

http://dx.doi.org/10.1002/cpe.3128

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.
EDITORIAL

Security of new generation computing systems

1. THIS SPECIAL ISSUE

Modern computing systems have become more easy-to-use, sophisticated and powerful, and have dramatically changed the way we live. However, the same systems add complexity and also introduce new interdependencies, vulnerabilities and privacy issues. There will be more ways to disrupt our life through cyber attacks. It is thus of great importance to consider and develop methods to mitigate those security risks. This special issue presents the recent advances on the security of new generation computing systems including distributed, cloud, and grid systems.

We are pleased to present to you nine technical papers dealing with cutting-edge research and technology related to this topic. These papers were selected out of the significantly extended versions of the 173 submissions from 28 countries in the 6th International Conference on Network and System Security (NSS 2012) and a large number of open submissions. The selection has been very rigorous, and only the best papers were selected.

In the first paper, ‘Impossible Differential Cryptanalysis on Cipher E2’ [1], Wei et al. present a series of six-round impossible differential characteristics of Cipher E2 with/without IT/FT functions. Based on these impossible differentials, the immunity of E2 against impossible differential cryptanalysis is evaluated.


The third paper, ‘Public-Key encryption Scheme with Selective Opening Chosen-Ciphertext Security based on the Decisional Diffie–Hellman assumption’ [3], presents a new result on the design of public-key encryption. Liu et al. propose a public key encryption scheme with full-fledged chosen-ciphertext security in selective opening setting directly from the Decisional Diffie–Hellman assumption. The security reduction is tight, and the scheme is free of chameleon hashing.

In the fourth paper, ‘On the Linear Complexity of Generalized Cyclotomic Binary Sequences of Length $2pq$’ [4], Chang et al. construct a new class of generalized cyclotomic binary sequences with period of $2pq$. The linear complexity and minimal polynomials of proposed sequences are determined. The results show that such sequences of length $2pq$ possess high linear complexity, which may be useful in stream cipher and communication domains.

The existing SCAs for the reverse engineering depend on the leakage models in a large extent and mainly focus on the single component of the algorithms, whereas the other parts of the target algorithm are known. In ‘Power Analysis Based Reverse Engineering on the Secret Round Function of Block Ciphers’ [5], Tang et al. propose a new reverse analysis method to reduce the dependency on the leakage models, which can be combined with the structure cryptanalysis to reverse the internal parameters of the linear and the nonlinear operations. The method uses the strict avalanche criterion for the nonlinear operations of block ciphers and applies the power analysis to reverse the structure parameters. The approach can achieve reverse analysis on the unknown round function of block ciphers.

To reduce the influence of key exposure, Li et al. introduce key-insulated mechanism into certificate-based cryptography and formalize the notion and security model of the certificate-based key-insulated signature scheme in ‘Provably Secure Certificate-based Key-Insulated Signature Scheme’ [6]. The authors present a certificate-based key-insulated signature scheme, which is proven to be existentially unforgeable against adaptive chosen message attacks in the random oracle model. The proposed scheme has several potential applications in trusted computing.
The Extensible Authentication Protocol (EAP) framework aims to realize a flexible authentication for wireless networks. In the seventh paper, ‘Efficient and Robust Identity-Based Handoff Authentication for EAP-Based Wireless Networks’ [7], Han et al. present a new identity-based handoff authentication scheme in which a special double-trapdoor chameleon hash function is used. The proposed scheme eliminates the assumption that the private key generator is fully trusted, which satisfies robust security properties and enjoys desirable efficiency.

In the eighth paper, ‘(Strong) Multi-Designated Verifiers Signatures Secure Against Rogue Key Attack’ [8], Au et al. study digital signatures that are verifiable by a specific set of verifiers as known as multi-designated verifiers signatures. They propose a scheme that is unforgeable under rogue key attack. In addition, they present a generic method which grants better privacy to the signer. This paper presents substantial advancements in the research area of digital signatures, a fundamental tool in providing data integrity, authenticity, as well as non-repudiation.

In the ninth paper, ‘Attack via Record Multiplicity on Cancelable Biometrics Templates’ [9], Li and Hu point out the vulnerability of cancelable biometrics and launch concrete attack methods over four typical cancelable fingerprint templates design algorithms. As cancelable biometrics is a prevalent biometric template protection scheme, the results of this paper trigger new security performance metric and design principle to address the security issue.

We sincerely hope that you will enjoy reading these papers in this special issue. We thank all the international reviewers for their professional services. We deeply thank Professor Geoffrey Fox, the Editor-in-Chief, for providing this opportunity to publish this special issue. With his continuous support, encouragement, and guidance throughout this publishing project, this special issue has been very successful.

REFERENCES


Li Xu
Fujian Normal University, China
E-mail: xuli@fjnu.edu.cn

Elisa Bertino
Purdue University, USA

Yi Mu
University of Wollongong, Australia