Journal of Computer Security 21 (2013) 599–600
DOI 10.3233/JCS-130483
IOS Press

Guest Editor's preface

Special Issue: Advances in Security for Communication Networks

The success of the Internet and of communication networks in general, opened new intriguing challenges for protocol designers. Consider, for example, the classic notion of "secure computation" introduced and achieved in the seminal works of Yao and of Goldreich, Micali and Wigderson. While such a notion considers only the stand-alone setting, where parties are connected to each other but isolated from the rest of the world, security in communication networks is more demanding. Indeed, when parties are connected to a network (i.e., parties can run several instances of protocols concurrently), secure computation has been proved impossible to achieve. Therefore, achieving information security in communication networks required to solve various open problems. New security notions have been introduced in order to better model real-world scenarios. New hardness assumptions have been used in order to enable the construction of more powerful cryptographic primitives. New security protocols and proof techniques have been developed in order to defeat network attacks mounted by malicious adversaries.

This special issue of the *Journal of Computer Security* includes six papers that cover various aspects of such recent challenges in information security in communication networks.

The paper "5PM: Secure pattern matching" by Joshua Baron, Karim El Defrawy, Kirill Minkovich, Rafail Ostrovsky and Eric Tressler addresses a popular problem in information security: secure pattern matching. The authors focus on the specific case of single-character wildcards and substring matching. They show a protocol called 5PM that outperforms previous constructions.

The paper "Short blind signatures" by Olivier Blazy, Georg Fuchsbauer, David Pointcheval and Damien Vergnaud introduces an improved form of blind signatures. Blind signatures are signatures of messages that remain hidden to the signer. They have various applications (e.g., e-cash). The construction given by the authors focuses on short signatures obtained with minimal interactions.

The paper "Field switching in BGV-style homomorphic encryption" by Craig Gentry, Shai Halevi, Chris Peikert and Nigel P. Smart proposes a general field-switching transformation that can be used to outperform previous transformations needed in homomorphic encryption schemes. Such schemes are a powerful tool in client-server applications and certainly represent one of the main novelties in Cryptography.

The paper "A more efficient computationally sound non-interactive zero-knowledge shuffle argument" by Helger Lipmaa and Bingsheng Zhang shows an improved construction of a non-interactive zero-knowledge proof for shuffle arguments, a classical network problem. Such arguments are used in some relevant applications (e.g., e-voting) when mix servers shuffles ciphertexts.

The paper "Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness" by Steven Myers, Mona Sergi and abhi shelat focuses on another typical attack on encryption schemes in communication networks: the man-in-the-middle attack, where the adversary aims at mauling a ciphertext. The authors show how to obtain non-malleable encryption against adaptive attacks (i.e., NM-CCA1) from plaintext-aware encryption schemes that are weakly simulatable.

The paper "Publicly verifiable ciphertexts" by Juan González Nieto, Mark Manulis, Bertram Poettering, Jothi Rangasamy and Douglas Stebila studies encryption schemes that guarantee two levels of security. Stronger security (i.e., IND-CCA2) is guaranteed when ciphertexts are observed in a fully untrusted environment, while milder security (i.e., IND-CPA) is guaranteed when ciphertexts are filtered by a gateway and then sent to the recipient. Such schemes achieve a reduced decryption cost still guaranteeing sufficient security in practical applications.

Acknowledgments

This special issue is the result of the joint work of many people and as a guest editor I am very grateful to all of them. I would like to thank the authors for submitting their excellent works to this special issue and for providing timely responses to my requests. I am very thankful to external reviewers for helping me in evaluating the submitted papers and for suggesting various improvements to the authors. I am very grateful to the JCS Editors-in-Chief, Andrew Myers and Pierangela Samarati, whose guidance significantly simplified my job, and to Kim Willems of IOS Press, who took care of the publication phase.

Ivan Visconti
Guest Editor
University of Salerno
Italy
E-mail: visconti@unisa.it