Security and privacy of electronic health information systems

Elisa Bertino¹ · Robert H. Deng² · Xinyi Huang³ · Jianying Zhou⁴

Published online: 27 October 2015
© Springer-Verlag Berlin Heidelberg 2015

1 Security and privacy of e-health systems

Digital technologies have dramatically transformed our daily lives by bringing countless conveniences and benefits. As an evolving concept, electronic health information has become the focus of attention in both academia and industry. By leveraging modern digital technologies like the internet and the cloud, electronic health information systems will be a key enabling technology in improving the quality and convenience of patient care, encouraging patient participation in their care, reducing medical errors, improving practice efficiencies, and saving time and cost. The complexity of electronic health information systems, however, raises several new security and privacy issues. It is thus critical to investigate and develop security and privacy mechanisms able to mitigate the emerging adversarial activities and meet

specific requirements of electronic health information systems.

2 The papers

There are two papers in this special section of International Journal of Information Security.

Huiling Qian, Jiguo Li, Yichen Zhang, and Jinguang Han in their paper entitled “Privacy preserving personal health record using multi-authority attribute-based encryption with revocation” introduce a new approach to preserve security and privacy in personal health record (PHR) service. Storage of PHRs is often outsourced to cloud service providers, which may expose very sensitive data like patient’s disease. To assure the security of PHR services, they introduce multi-authority attribute-based encryption (ABE) in the context of PHR services. Before outsourcing PHRs to third parties, patients first use ABE to encrypt the data. As a result, cloud service providers and unauthorized users cannot access patient’s PHRs. By using ABE to encrypt data, the proposed approach supports fine-grained access control, which makes it more practical and functional. Such new scheme also supports efficient on-demand user/attribute revocation and dynamic policy update, which incurs low overhead for patients when updating access control policies or revoking authorized users. The authors organize the system into two types of domain: personal domain (PSD) and public domain (PUD). In PSDs, key-policy ABE is used to encrypt data and patients are responsible for generating and issuing secret keys. In PUDs, ciphertext-policy ABE is used to encrypt data and patients only need to specify a policy and combine the policy with the ciphertext.

Bo Qin, Hua Deng, Qianhong Wu, Josep Domingo-Ferrer, David Naccache, and Yunya Zhou in their paper

✉ Elisa Bertino
bertino@purdue.edu

Robert H. Deng
robertdeng@smu.edu.sg

Xinyi Huang
xyhuang81@gmail.com

Jianying Zhou
jyzhou@i2r.a-star.edu.sg

¹ Department of Computer Science, CERIAS and Cyber Center, Purdue University, West Lafayette, IN 47907-2107, USA

² School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902, Singapore

³ School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350117, Fujian, China

⁴ Infocomm Security Department, Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, South Tower, Singapore 138632, Singapore

entitled “Flexible attribute-based encryption applicable to secure e-healthcare records” introduce a flexible encryption approach to secure personal healthcare records in electronic health information systems. Their paper presents a comprehensive review of attribute-based encryption systems in the literature and points out a drawback of the key-policy attribute-based encryption (KP-ABE) in its application to electronic health information systems. To address this issue, they propose a dynamic ABE paradigm, referred to as access policy redefinable ABE (APR-ABE). APR-ABE distinguishes itself from other KP-ABE schemes by allowing users to redefine their access policies and delegate keys for the redefined ones, so that a priori access policies are no longer mandatory. Unlike other delegatable ABE, APR-ABE does not require the redefined access policies to be more restrictive than the original ones in key

delegation. The authors present the APR-ABE framework where all attributes are organized in a matrix and users’ access policies are defined over attribute vectors. Following this framework, the authors construct an APR-ABE scheme with short ciphertexts. Because of the use of attribute vectors, new attributes can be added into access policies without having to make the refined policies more restrictive. The paper describes how APR-ABE can be employed in electronic health information systems to achieve flexible access control on personal health records.

Acknowledgments We would like to express our gratitude to the Editors of the Springer’s International Journal of Information Security, for giving us the opportunity to prepare this special section. In addition, we sincerely thank the reviewers for their time and effort on reviewing papers and all authors for their contributions.