Efficient And Deniable Authenticated Encryption

SPEAKER **Prof Kasper Bonne RASMUSSEN**

Associate Professor
Department of Computer Science
University of Oxford
United Kingdom

DATE 9 May 2017 (Tuesday)
TIME 2:00 pm - 3:00 pm
VENUE CS Seminar Room, Y6405, 6th Floor
Yellow Zone, Academic 1
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Consider a scenario in which a whistleblower (Alice) would like to disclose confidential documents to a journalist (Bob). Bob wants to verify that the messages he receives are really from Alice; at the same time, Alice does not want to be implicated if Bob is later compelled to (or decides to) disclose her messages, together with his secret key and any other relevant secret information. To fulfill these requirements, Alice and Bob can use a deniable authenticated encryption scheme. In this talk we formalize the notions of strong- and weak deniable authentication, and discuss the relationship between these definitions. Although the terms strong- and weak deniability have been used before in the cryptographic literature, they have not been formally defined for encryption schemes. We show that Bob can still securely authenticate messages from Alice after all his secret information is revealed to the adversary only when using a weakly (but not strongly) deniable scheme. We refer to this ability as post-compromise message authentication. We present two efficient encryption schemes that provide deniable authentication. Both schemes incur overhead similar to that of non-deniable schemes. As such, they are suitable not only when deniability is needed, but also as general encryption tools. We provide details of the encryption, decryption, forgery and key-generation algorithms, and formally prove that our schemes are secure with respect to confidentiality, data authentication, and strong- and weak deniable authentication. We have made implementations of our schemes available as stand-alone command line tools, written in Python. We characterize the performance (both time- and space complexity) of these implementations, and show that our schemes incur very limited ciphertext expansion and computation overhead compared to standard asymmetric encryption.

BIOGRAPHY

Kasper Rasmussen is Associate Professor in the Computer Science Department at the University of Oxford. He joined the university in 2013 and in 2015 was awarded a University Research Fellowship from the Royal Society in London. Kasper Rasmussen completed his master's degree in Computer Science (Information technology and Mathematics) from the Technical University of Denmark (DTU) in December 2005. His master's thesis was on optimization of path protection in circuit switched networks. Kasper did his Ph.D. with Prof. Srdjan Capkun at the Department of Computer Science at ETH Zurich. During his Ph.D. he worked mainly on security issues relating to secure time synchronization and secure localization with a particular focus on distance bounding. After completing his Ph.D., Kasper worked as a post-doc at University of California, Irvine, with Prof. Gene Tsudik for a few years before joining University of Oxford.

All are welcome!

In case of questions, please contact Dr WONG Hau San Raymond at Tel: 3442 8624, E-mail: cshswong@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.