香港浸會大學
HONG KONG BAPTIST UNIVERSITY

DEPARTMENT OF
COMPUTER SCIENCE
計算機科學系

ONLINE SEMINAR
2021 SERIES

Department of Computer Science

Dr. Wanli Xue

Senior Research Associate
Cyber Security Cooperative Research Centre
School of Computer Science and Engineering
University of New South Wales, Australia

Date: 27 May 2021 (Thursday)
Time: 2:00pm – 3:00pm GMT+8 (HKT)

*Zoom details will only be provided to registrants

Towards A Compressive-Sensing-Based Lightweight Encryption Scheme for the Internet of Things

ABSTRACT

Internet of Things (IoT) is flourishing and has penetrated deeply into people's daily life. With the seamless connection to the physical world, IoT provides tremendous opportunities to a wide range of applications. However, potential risks exist when the IoT system collects sensor data and uploads it to the Cloud. The leakage of private data can be severe with curious database administrator or malicious hackers who compromise the Cloud. In this work, we propose Kryptein, a compressive-sensing-based lightweight encryption scheme for Cloud-enabled IoT systems to secure the interaction between the IoT devices and the Cloud. Kryptein supports random compressed encryption, statistical decryption, and accurate raw data decryption. According to our evaluation based on two real datasets, Kryptein provides strong protection to the data. It is 250 times faster than other state-of-the-art systems and incurs 120 times less energy consumption. The performance of Kryptein is also measured on off-the-shelf IoT devices, and the result shows Kryptein can run efficiently on IoT devices. After comparing with other state-of-the-art lightweight ciphers on IoT (Simon and Speck), IoT system with Kryptein is expected to have a much more longevity with about 35% extended lifetime. Further, experiments illustrated IoT data variance will not affect Kryptein's accuracy in a long term usage, and Krpytein is also able to support basic analytics tasks like machine learning (e.g., classification).

BIOGRAPHY

WANLI XUE received the Ph.D. degree from the School of Computer Science and Engineering, University of New South Wales, Australia. He is currently a Senior Research Associate with the Cyber Security Cooperative Research Centre (CSCRC), and the School of Computer Science and Engineering, University of New South Wales. His research interests include security and privacy issues in cyber physical systems and the IoT, including highly efficient privacy-preserving techniques for the IoT and IoT-related sensing systems and data analytic services.

ENQUIRY

Tel: 3411-2385 Email: comp@comp.hkbu.edu.hk Website: https://www.comp.hkbu.edu.hk/v1/?page=seminars