RESEARCH SEMINAR

Searchable Symmetric Encryption and Its Attacks

Dr Kaitai LIANG
Tenured Faculty Member
Cybersecurity Group
Delft University of Technology
The Netherlands

Date : 4 Jun 2024 (Tue)
Time : 3:00 pm - 4:00 pm
Venue : HJ303

Abstract

Searchable Symmetric Encryption (SSE) represents an intriguing technique that empowers users to delegate keyword searches over encrypted databases to an honest-but-curious server. The primary goal is to uphold the confidentiality of both the keywords and the encrypted documents. A comprehensive understanding of SSE entails navigating through the intricacies of how it facilitates secure and privacy-preserving searches within the realm of encrypted data. In this talk, we will embark on a detailed exploration of SSE's underlying concepts, mechanisms, and the intricate security notions that serve as the foundation for this cryptographic technique. Acknowledging that no cryptographic protocol is impervious to vulnerabilities, the discussion will delve into an examination of current attacks on SSE. This aims to deepen comprehension of the strengths and limitations inherent in SSE, a critical aspect for its ongoing development and effective deployment in real-world applications. At last, the talk will shed light on some of the open challenges associated with SSE.

About the Speaker

Dr Liang is a tenured faculty member in the Cybersecurity group at Delft University of Technology. His research, featured in international information security journals and conferences like USENIX Security, NDSS, Asiacrypt, ESORICS (with a best research paper award), IEEE TIFS, and IEEE TDSC, addresses cybersecurity challenges using information security and cryptographic tools. As a principal investigator in various EU funded projects, he has demonstrated real-world security impact through collaborations with academic and industrial partners. Dr. Liang has served TPC member, General Chair, and Steering Committee for international security and privacy conferences, e.g., USENIX Security, IEEE Euro S&P, ESORICS, IEEE CSF, and PoPETs, and an Associate Editor for international journals such as the Computer Journal, IEEE Transactions on Artificial Intelligence, and the EURASIP Journal on Information Security. He has also contributed to ISO standards as a member of the standards committee 381027 "Cybersecurity & Privacy" at NEN.

WE DRIVE INNOVATION THROUGH
SMART COMPUTING

Background Image: Technology Vectors by Vecteezy