UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Privacy-Preserving and Functional Information Systems

by

Thang Hoang

For the Ph.D. degree in Computer Science and Engineering

Information systems generally involve storage and analytics of large-scale data, many of which may be highly sensitive (e.g., personal/medical information, financial transactions). Thus, it is critical to ensure that these systems not only provide essential functionalities at large scale efficiently but also achieve a high level of security against potential cyber threats. Unfortunately, there are significant research challenges in offering security and privacy for such information systems while preserving their original functionalities and efficiency (e.g., search, update, analytics). Hence, there is a critical need for efficient cryptographic protocols that can address data privacy versus utilization dilemma for real-life applications.

In this talk, we will present our new series of privacy-enhancing technologies toward enabling breach-resilient and functional information systems. We target privacy-preserving data outsourcing applications featuring critical functionalities (i.e., data query, access control) with a high level of privacy. Specifically, we will present our proposed oblivious access techniques that permit the client to hide the access patterns efficiently when accessing data remotely in the presence of active adversaries. We will then introduce our new oblivious data storage platform, which harnesses Trusted Execution Environment (TEE) such as Intel-SGX to enable concurrent access from multiple users over the shared database with high throughput, low latency and high level of privacy guarantee (e.g., confidentiality, integrity and concealed access pattern).

Examining Committee
Morris Chang, Ph.D., Chairperson
Attila A. Yavuz, Ph.D., Major Professor
Jean-François Biasse, Ph.D.
Jay Ligatti, Ph.D.
Xinming (Simon) Ou, Ph.D.
Mike Rosulek, Ph.D.

Friday, April 17, 2020
1:30 PM
Online (Collaborate Ultra):
Email hoangm@mail.usf.edu for more information

THE PUBLIC IS INVITED

Publications

1) **Thang Hoang**, Jorge Guajardo, Attila A. Yavuz, "MACAO: A Maliciously-Secure and Client-Efficient Active ORAM Framework", in NDSS, 2020.
2) **Thang Hoang**, Rouzbeh Behnia, Yeongjin Jang, Attila A. Yavuz, "MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves", in 20th ACM CODASPY, 2020.
3) **Thang Hoang**, Attila A. Yavuz, Jorge Guajardo, "A Multi-server ORAM Framework with Constant Client Bandwidth Blowup". ACM Transactions on Privacy and Security, 2019.
4) **Thang Hoang**, Attila A. Yavuz, F. Betül Durak, Jorge Guajardo, "A Multi-Server Oblivious Dynamic Searchable Encryption Framework". Journal of Computer Security, 2019.
5) **Thang Hoang**, Muslum O. Ozmen, Yeongjin Jang, Attila A. Yavuz, "Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset", in 19th PETS, 2019.
6) **Thang Hoang**, Attila A. Yavuz, Jorge Guajardo, "A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services". IEEE Transactions on Services Computing, 2019.
7) **Thang Hoang**, Ceyhun D. Ozkaptan, Gabriel Hackebeil, Attila A. Yavuz, "Efficient Oblivious Data Structures for Database Services on the Cloud". IEEE Transactions on Cloud Computing, 2019.
8) **Thang Hoang**, Attila A. Yavuz, F. Betül Durak, Jorge Guajardo, "Oblivious Dynamic Searchable Encryption on Distributed Cloud Systems", in 32nd IFIP DBSec, 2018.
9) Muslum O. Ozmen, **Thang Hoang**, Attila A. Yavuz, "Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search", in IEEE ICC, 2018.
10) **Thang Hoang**, Ceyhun D. Ozkaptan, Attila A. Yavuz, Jorge Guajardo, Tam Nguyen, "S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing", in 24th ACM CCS, 2017.
11) **Thang Hoang**, Attila A. Yavuz, Jorge Guajardo, "Practical and Secure Dynamic Searchable Encryption via Oblivious Access on Distributed Data Structure", in 32nd ACSAC, 2016.

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.