Secure Searching

Professor David Cash
Rutgers University, Department of Computer Science

9/12/2017 at 10:30 am
CoRE A 301

Abstract

Storing data securely while enabling efficient queries on that data is a challenging, multifaceted problem. Standard encryption can provide strong confidentiality but completely disables non-trivial querying by parties who cannot decrypt. Moreover, strongly isolating tenants in shared systems poses further complications.

This talk presents my work on designing and analyzing methods to efficiently and securely query data. In the first part, I will cover my work on searchable encryption, including empirical security analyses of prior industry-used searchable encryption, a better construction of searchable encryption that became the basis of a more secure industry product, and a foundational lower bound on the main performance bottleneck of my construction.

In the second part, I will present my recent work on the security of the industry-standard approach to enabling full-text search in multi-user services. I will show that multi-tenant indexes fail to sufficiently isolate users by exhibiting a novel side channel in relevance scores and then developing techniques for exploiting the side channel in practice. This new attack is effective against a multiple cloud service providers, including a major service with millions of users. Finally I will conclude with countermeasures.

Bio

David Cash is an assistant professor in the Department of Computer Science at Rutgers University. Prior to joining Rutgers, he was a post-doc in the Cryptography Group at IBM Research, at Ruhr University Bochum, and at University of California, San Diego. He earned his Ph.D from Georgia Tech in 2009. His research in cryptography and security spans theoretical and experimental perspectives and was recognized with an NSF CAREER Award and the EUROCRYPT Best Paper Award in 2010 and 2011.

Faculty Host: Thu Nguyen