Securing Web Applications with Predicate Access Control

PI: Kirill Levchenko
Presenter: Zhaoma Zhang

Abstract:
Web application security is an increasingly important concern as we entrust these applications to handle sensitive user data. Security vulnerabilities in these applications are quite common, however, allowing malicious users to steal other application users' data. A more reliable mechanism for enforcing application security policies is needed. Most applications rely on a database to store user data, making it a natural point to introduce additional access controls. Unfortunately, existing database access control mechanisms are too coarse-grained to express an application security policy.

In this talk, we present a fine-grained access control mechanism for controlling access to user data. Application access control policy is expressed using row-level access predicates, which allow an application's access control policy to be extended to the database. These predicates are expressed using the SQL syntax familiar to developers, minimizing the developer effort necessary to take advantage of this mechanism. We implement our predicate access control system in the PostgreSQL 9.2 DBMS and evaluate our system by developing an access control policy for the Drupal 7 and Spree Commerce. Our mechanism protected Drupal and Spree against five known security vulnerabilities.

Bio:
I am a first-year PhD student from CSE department of UCSD advised by Dr. Kirill Levchenko. I'm interested in security in general and currently I'm working on usable security from developers' perspective.