Privacy Aspects in Data Querying

Michael Segal

Communication Systems Engineering Department
Ben-Gurion University of the Negev, Beer-Sheva, Israel
segal@bgu.ac.il

Abstract. Vast amounts of information of all types is collected daily about people by governments, corporations and individuals. The information is collected, for example, when users register to or use online applications, receive health related services, use their mobile phones, utilize search engines, or perform common daily activities. As a result, there is an enormous quantity of privately-owned records that describe individuals finances, interests, activities, and demographics. These records often include sensitive data and may violate the privacy of the users if published.The common approach to safeguarding user information, or data in general, is to limit access to the storage (usually a database) by using and authentication and authorization protocol. This way, only users with legitimate permissions can access the user data. However, even in these cases some of the data is required to stay hidden or accessible only to a specific subset of authorized users. Our talk focuses on possible malicious behavior by users with both partial and full access to queries over data. We look at privacy attacks that meant to gather hidden information and show methods that rely mainly on the underlying data structure, query types and behavior, and data format of the database. The underlying data structure may vary between graphs, trees, lists, queues, and so on. Each of these behaves differently with regards to data storage and querying, allow for different types of attacks, and require different methods of defense. The data stored in databases can be just about anything, and may be a combination of many different data types such as text, discrete numeric values, coordinates, continuous numeric values, timestamps, and others. We will show how to identify the potential weaknesses and attack vectors for each of these combinations of data structures and data types, and offer defenses against them. This is a joint work with Eyal Nussbaum.