SemInar

Department of Computer Science

Dr. Shiva Houshmand

Assistant Professor, Department of Computer Science

Using Personal Information for Targeted Password Cracking Attacks

Date: Wednesday, November 16, 2016
Time: 2:00 – 3:00 p.m.
Location: EGRA309C, CS Conference Room

Abstract

Passwords continue to be the primary means of authentication and security for online accounts and use in encrypting files and disks. Despite recommendations of security experts, people still reuse their passwords across different websites. Also when forced to change their passwords they slightly change them by add/removing simple characters. The attacker can then target a specific user and improve his attack by incorporating personal information and passwords of the user from other websites. Current password cracking tools and techniques do not have the capability of considering personal information or previous passwords of a specific user at the time of guessing.

In this work we explore how an attacker can use knowledge of a user's previous password and other personal information systematically to improve a password cracking task. We focus on the dictionary-based probabilistic context-free grammar (PCFG) approach to password cracking that trains on revealed password sets and then uses the learned grammar to generate guesses in optimal probability order. We show that we can effectively incorporate personal information about a target into the PCFG password cracking system in a very straight forward manner to assist in a targeted attack. We first develop a mathematical model of merging multiple grammars that combines the characteristics of the component grammars. Then we show how various component grammars and dictionaries can be derived using personal information about the target. The resulting merged target grammar (also

merged with a standard grammar) and various target dictionaries generates guesses that more quickly match the target's password when personal information is used.