COLLOQUIUM

Shiva Houshmand

4-13-17

Neckers 156
Time: 3:00pm

RECEPTION IMMEDIATELY FOLLOWING IN THE MATH LIBRARY.

Abstract: Passwords are critical for security in many different domains such as social networks, emails, encryption of sensitive data and online banking. Human memorable passwords are thus a key element in the security of such systems. It is important for system administrators to have access to the most powerful and efficient attacks to assess the security of their systems more accurately. In this talk I describe the recent techniques for password cracking and assessing the strength of passwords. The probabilistic context-free grammar technique has been shown to be very effective in password cracking. In this approach, the system is trained on a set of revealed passwords and a probabilistic context-free grammar is constructed. The grammar is then used to generate guesses in highest probability order, which is the optimal off-line attack. I also describe how entropy measures and Markov models have been used as password-strength meters to analyze the strength of user chosen passwords. A new password meter will also be introduced that estimates the probability of passwords being cracked. The system modifies the weak password slightly and suggests a new stronger password to the user. By dynamically updating the grammar we make sure that the guessing entropy increases and the suggested passwords thus remain resistant to various attacks.

Modern Techniques in Password Cracking and Password Meters

SIU CARBONDALE Southern Illinois University