Password Cracking: Jyvaskyla Summer School

Course Outline

August 5-7, 2015

Instructor: Sudhir Aggarwal

Day 1

Morning

L1 – Introduction (approx. ½ hour)

Overview of the course. Access to Lectures, Course Outline and Exercises. Download Datasets.zip folder: contains a Dictionaries Folder (5 .txt files) and 2 files: yahoo_test.txt and myspace_hashes.txt. Also download checkPass.zip folder: contains checkPass.cpp and a makefile.

L2 – Hashing (approx. 1 hours)

What is hashing, cryptographic hashes and properties, types of hashing algorithms (LM, NMTL, MD5, etc.) storing, salting, locating on media.

L3 – Cracking Overview (approx.1 hours)

Dictionary based attacks, mangling rules, brute forcing, Markov models, and rainbow tables

Afternoon

E1a – Exercise 1: Introduction to John the Ripper (1 hours)

Instructor: Help in setting up John the Ripper and Exercise 1.

E1b – Student Exercise 1: Introduction to John the Ripper (1 1/2 hours)

Students: Downloading and setting up the environment and completing Exercise 1.

L4 – Overview – Probabilistic Context-free Grammars (11/2 hour)

Grammars, context-free grammars, derivations, trees, probabilistic aspects and consistency, ambiguity and problems.

Day 2

Morning

L5 – Grammar-based Probabilistic Password Cracking PPC (1 hour)

Introduction to our cracking systems and basic capabilities.

E2a – Exercise 2, part 1(using PPC) (1 hour)

Instructor: Demo and explanations of using PPC for training: options, source files, output. Understanding output folders and related information. Understanding training sets and training dictionaries. Main discussion on PPC and some aspects of NPC. Some discussion on cracking / guessing with a brief demo.

L6 – Details of Training and Cracking (1 hour)

Some details / code related to training and cracking, including algorithms (Pivot, Deadbeat Dad), data structures used and use of multiple dictionaries.

Afternoon

E2 b – Student Exercise 2, part 2 (2 hours)

Students do Exercise 2 to experiment with John the Ripper and explore various ways and modes to crack a hash file.

L7 – Modeling Differences (1 hour)

Talk on how PPC/NPC can generate better guesses if previous information about a target can be used such as a previous password or other user data.

L7b – Demo of Modeling Differences (1 hour)

As time permits, instructor will show how the new grammars for modelling differences are generated.

Day 3

Morning

L8 – New Capabilities: Keyboard, Multiwords and Dictionaries: NPC (2 hours)

A talk on the new capabilities of our cracking system (called NPC) and its effectiveness.

L9 – Building Better Passwords (1 hour)

A talk on how one can use our cracking approach to provide uses with better passwords.

Afternoon

E3 – Student Exercise 3 (2 hours)

A more detailed exercise building on the previous exercises. Students will use John the Ripper and see how they can generate guesses most effectively on a target Yahoo test file. Instructor will do the same using NPC but using the full capabilities of the probabilistic grammars as well as the improved dictionaries.

L10 – Applications – Passwords on Disk (1 hour)

If passwords are stored on disk, how can we create a list of the most likely strings to be passwords?

Review and Wrap up (1 hour)

Review and Final Questions. Open session.