L1:
Password Cracking
Introduction

Sudhir Aggarwal and Shiva Houshmand
Florida State University
Department of Computer Science
E-Crime Investigative Technologies Lab
Tallahassee, Florida 32306
August 5-7, 2015

Course Information

- Title: Password Cracking
- Course Instructors: Sudhir Aggarwal, Shiva Houshmand
- August 5-7, 2015, Jyvaskyla Summer School
- Approximately 5 hours Lecture, 2 hours lab / exercises per day
- Credits: 2
- Prerequisites: some programming, algorithms and data structures, some UNIX, probability
- Level: graduate, pass/fail
- Short report on what you learned and your accomplishments

Course Abstract

- We cover both the theory and the practice of password cracking.
- Survey the basic ideas of how passwords are stored and what it means to crack a password.
- Cover a prominent open source password cracking system called John the Ripper and cover its model, operation and use.
- Cover our own probabilistic password cracking approach developed in the ECIT Laboratory at Florida State University.

Course Abstract Continued

- PPC / NPC Theoretical Basis
  - Probabilistic context-free grammars
  - Training the grammars
  - Generating guesses in highest probability order.
  - Learning Patterns
- Labs & exercises using John the Ripper – students
- Labs & exercises using PPC / NPC - instructors

History of PPC Work at ECIT

- Initial Concepts Explored
- Basic Model and Implementation
- Advanced Model and Implementation
- Related Research
  - Better passwords, identifying passwords, targeted attacks

Contributors to PPC Work

- M. Weir, Sudhir Aggarwal, Breno de Medeiros, Bill Glodek, “Password cracking using probabilistic context free grammars,” *Proceedings of the 30th IEEE Symposium on Security and Privacy*, May 2009, pp. 391-405.
- M. Weir, S. Aggarwal, M. Collins, and H. Stern, “Testing metrics for password creation policies by attacking large sets of revealed passwords,” *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*, October 4-8, 2010, pp. 163-175.
- Shiva Houshmand, Sudhir Aggarwal, “Building better passwords using probabilistic techniques,” *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC ’12)*, December 2012, pp. 109-118.
- Shiva Houshmand, Sudhir Aggarwal, Umit Karabiyik, “Identifying Passwords Stored on Disk,” *Advances in Digital Forensics XI, eds. Peterson & Shenoi, Springer, (Proceedings 11th IFIP WG11.9 International Conference)*, January 2015.
- Houshmand, S.; Aggarwal, S.; Flood, R., "Next Gen PCFG Password Cracking," *Information Forensics and Security, IEEE Transactions on , vol.10, no.8*, pp.1776,1791, Aug. 2015

Lectures, Exercises, Files

- Lectures Folder (.pdf)
  - Course Outline
  - Lectures L1 – L10
  - Exercises
- Datasets Folder (.zip)
  - Dictionaries Folder
  - Some .txt files
- checkPass Folder (.zip)