Distributed password cracking with Condor and John the Ripper

Emir Imamagic Aco Dmitrovic Stjepan Buljat

Department of Computer Systems,
University Computing Centre, Croatia
{eimamagi, aco, sbuljat}@srce.hr

Username/Password pair is commonly used method for user authentication. Password is a word that consists of letters, numbers and special characters. When registering to system, user chooses the password and system stores it in a safe manner.

Systems must provide sound password storing mechanism in order to prevent unauthorized access to the system. Usually, systems use some hashing algorithm (e.g. MD5, SHA1) for storing passwords. On the other hand, it is the responsibility of users to choose reasonably complex passwords. Otherwise, the security of whole system can be compromised. Administrators usually define rules for creating passwords and insist on periodical password changing. In some cases, administrators choose to check quality of stored passwords.

Password cracking is a process of recovering passwords from the safe system format. It consists of guessing the password, converting it to the stored format and comparing with stored value. There are several techniques for cracking passwords: guessing, dictionary attack and brute force. Guessing approach uses information about users, such as birthday and login name to guess the password. Dictionary attack uses words from dictionary of user's native language or some other languages. Brute force approach uses every possible value of password. Since the number of possible values is large, this approach cannot be performed in reasonable period.

Password cracking can be easily distributed in order to speed up the process. Process can be divided in several tasks that perform a part of the job. In case of brute force approach, task can cover set of possible passwords. In case of dictionary attack, task can process part of the dictionary. If the password list is large, one task can process set of passwords.

John The Ripper is a well known password cracker. It can crack password stored by various systems. Currently supported are: 11 flavors of UNIX, DOS, Win32, BeOS, OpenVMS, Windows NT/2000/XP/2003, Kerberos AFS and MySQL. John enables usage of all three techniques described above. In case of brute force cracking, it uses character frequency tables in order to improve performance.

Condor is an open source project of University of Wisconsin. Condor is designed specifically for high throughput computing (HTC) and CPU harvesting. CPU harvesting is process of exploiting non-dedicated computers (e.g. desktop computers) when they are

not used. Users describe their applications with simple language and submit them to Condor. Condor then finds free resources and executes them. Condor also provides advance functionalities, such as storing the job status, fault recovery, submitting complex job workflows, job migration, retrieving detailed information about resource consumption and transferring files to/from remote machines.

Our main motivation for this work was to evaluate password quality compared with available password cracking technologies. Beside passwords format (e.g. length, used characters), our goal was to identify reasonable duration of password. Achieved results were used for improvement of security rules and policy.

We used John for password cracking and Condor to distribute the process on workstations. Tasks were distributed in a way that each task was processing set of passwords from a real server. In this case, we used all three cracking approaches. We also generated set of random passwords in order to benchmark Jack's brute force mode. In all cases, we got significant speed up, by using unoccupied workstations.