Abstract der fertigen Arbeit

Das in den letzten Jahren stetig wachsende Sicherheitsbewusstsein der Bevölkerung führt dazu, dass eine steigende Anzahl an Menschen von kryptographischen Verfahren Gebrauch macht und ihre lokal gespeicherten Daten verschlüsselt. Während diese Entwicklung aus Datenschutzgründen zu begrüßen ist, birgt sie auch einen negativen Nebeneffekt für die Verbrechensbekämpfung: IT-Forensikerinnen und IT-Forensiker sehen sich nun verstärkt vor das Problem gestellt, Informationen auf in Kriminalfällen sichergestellten Datenträgern nicht auswerten zu können, da diese vom Besitzer verschlüsselt wurden. Um diese für die Aufklärung des Falles wichtigen Beweismittel wieder zugänglich zu machen, besteht oft keine andere Möglichkeit als das unbekannte Passwort durch Ausprobieren aller Kombinationen aus Buchstaben, Zahlen und Zeichen zu erraten, was sich als eine äußerst rechen- und damit zeitintensive Aufgabe herausgestellt hat. Eine Alternative zu diesen sogenannten Brute-Force Attacken stellt die Verwendung von Passwortlisten dar, die viele verschiedene relativ simple und damit unsichere aber dennoch oft genutzte Passwörter beinhalten. Diese generischen Passwortlisten enthalten aber immer seltener das tatsächliche Passwort, da eine gängigere Methode bei der Generierung von Passwörtern das Einbinden von personenbezogenen Begriffen wie Namen, Orten oder Jahreszahlen ist.
In dieser Arbeit wird erforscht, nach welchen Mustern personenbezogene Passwörter aufgebaut sind und ob es möglich ist, automatisiert nach Informationen über eine Person zu suchen, um daraus Passwörter nach diesen Mustern zu erstellen. Zu diesem Zweck wurde ein Tool entwickelt, das nach Eingabe des Benutzernamens der Zielperson in sozialen Netzwerken automatisiert online nach persönlichen Informationen sucht und daraus eine personalisierte Passwortliste generiert. Es konnte gezeigt werden, dass die Erstellung von personenbezogenen Wortlisten und Regeln für den sogenannten Crackingprozess eine schnelle und erfolgsversprechende Alternative zu klassischen Brute-Force Attacken bildet.