On the Usability and Security of Password-Based User Authentication

Maximilian Golla

Die Benutzbarkeits- und Sicherheitsprobleme von Passwörtern werden seit Jahrzehnten untersucht. Dennoch sind Passwörter weiterhin das primäre Authentifizierungsmerkmal in Computersystemen. Mit der zunehmenden Anzahl von Diensten, für die eine Authentifizierung erforderlich ist, stehen Nutzer, Administratoren und Systementwickler vor neuen Herausforderungen, wie zum Beispiel der Bedrohung durch die Nutzung schwacher Passwörter oder die Wiederverwendung von Passwörtern. Um Nutzer besser zu schützen und passwortbasierte Authentifizierung zu stärken, haben Dienste neuartige Lösungen, die mehr als ein Authentifizierungsmerkmal berücksichtigen, entwickelt. Gleichzeitig verzögern Altlasten, wie etwa falsche mentale Modelle der Nutzer und Systementwickler über die Fähigkeiten von Angreifern, die Verbreitung sicherer Passwortpraktiken. In dieser Dissertation werden vier Schlüsselaspekte der passwortbasierten Benutzerauthentifizierung behandelt: Passwortwiederherstellung, Passwortstärkemeter, Benachrichtigungen zur Wiederverwendung von Passwörtern und crackingresistente Passwortmanager.

Zuerst betrachten wir das Themengebiet der Passwortwiederherstellung. Wenn Nutzer dazu gezwungen sind, komplizierte Richtlinien zum Aufbau oder Wechsel von Passwörtern zu erfüllen, darf man sie nicht dafür verantwortlich machen, dass sie ihre Passwörter vergessen. Derzeit bereitgestellte wissensbasierte Wiederherstellungsverfahren sind stark von den Vorlieben und der Auswahl der Nutzer beeinflusst und daher angreifbar. Wir schlagen deshalb ein Verfahren vor, das frei von Beeinflussungen durch dessen Nutzer ist, und Nutzer davon befreit sich ein Geheimnis zu merken und eine gute Leistung über längere Zeiträume aufweist.

Als Nächstes befassen wir uns mit Passwortstärkemetern. Bei der Kontoerstellung können Nutzer von zusätzlichen Hilfestellungen und Rückmeldung durch sogenannte Passwortstärkemeter profitieren. In einer groß angelegten Untersuchung fanden wir jedoch viele Stärkemeter, die ungenau arbeiten, obwohl sie auf beliebten Webseiten oder in Passwortmanagern zum Einsatz kommen. Um Entwickler und Systemdesigner zu unterstützen, bieten wir deshalb Metriken, Hilfestellungen und Werkzeuge zur Verbesserung der Stärkemeter an.

Anschließend untersuchen wir die Wiederverwendung von Passwörtern. Momentan ist die Wiederverwendung von Passwörtern eines der dringlichsten Sicherheitsprobleme bei der passwortbasierten Authentifizierung. Prophylaktische Überprüfungen durch die Dienstbetreiber anhand ihrer Benutzerdatenbank auf Übereinstimmungen mit gestohlenen und im Internet veröffentlichten Anmeldeinformationen sind eine Technik, mit der die Erfolgsquote von Passwortwiederverwendungsangriffen begrenzt wird. Die anschließende Kommunikation des Sicherheitsproblems mit dem Nutzer ist eine herausfordernde Aufgabe, da der gesamte Sachverhalt eine Komplexität darstellt, die für Nutzer nur schwer verständlich ist, jedoch sofortige Maßnahmen erfordern, um drohenden Schaden abzuwenden. Wir zeigen, dass die mentalen Modelle der Nutzer in Bezug auf die Bedrohung durch die Wiederverwendung von Passwörtern unvollständig und oftmals falsch sind. Im Anschluss entwickeln wir Hilfestellungen für Systementwickler zur Verbesserung ihrer Kommunikation mit dem Nutzer.

Zum Abschluss analysieren wir die Sicherheit von Passwortmanagern. Passwortmanager können dabei helfen, mit der steigenden Anzahl an Passwörtern und Konten umzugehen. Durch die Synchronisierung der passwortgeschützten Tresordatei mit Clouddiensten haben Angreifer jedoch eine höhere Chance den Tresor zu stehlen und erfolgreich zu entschlüsseln. Crackingresistente Passwortmanager helfen dieses Problem zu mindern, indem sie verschleiern, ob ein Rateversuch gegen das Masterpasswort richtig ist oder nicht. Wir zeigen, dass der aktuelle Vorschlag zur Konstruktion solcher Manager anfällig für verteilungsbasierte Angriffe ist, und schlagen eine sicherere Konstruktion vor.