

openHPI-Kurs „Digitale Identitäten“
Raten, Abgreifen, Wiederverwenden –
Angriffe auf Passwörter

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Universität Potsdam

Angriffe auf Passwörter

Passwortgestützte Authentifizierung wird häufig vermittels folgender Methoden von Hackern überwunden:

- **Raten** von Passwörtern
- **Knacken** von Passwörtern
 - **Systematisches Durchprobieren**, z.B. mit Wortlisten, Passwort-Top10-Listen, ...
- **Abfangen** von Passwörtern (Sniffing)
 - **Netzwerkpakete** werden abgefangen und nach Vorkommen von Benutzernamen und Passwörtern durchsucht
- Einsatz von **Keyloggern** und **Trojanern**, die das Opfersystem bei Passworteingabe belauschen
- **Social Engineering**

Erraten von Passwörtern (1/4)

- Passwörter werden online erraten und es wird direkt ausprobiert, unberechtigten Zugang zu einem Dienst im Internet zu erlangen
- Erraten von Nutzer/Passwort-Kombination ist überraschend oft erfolgreich, weil Nutzer zu einfache Passwörter verwenden und Passwörter wiederverwenden
- Bequemlichkeit bei der Nutzung führt zur Vernachlässigung der Sicherheit
 - einfache Passwörter sind leicht zu merken, aber auch leicht zu erraten ...

Erraten von Passwörtern (2/4)

Finden gültiger Nutzernamen

Erratene Passwörtern sind für die Angreifer nur nützlich, wenn auch zugehöriger gültiger Benutzername gefunden wird

- Verwendung häufig vorkommender Nutzernamen, z.B.
 - admin, gast, service, ...
- Verwendung von Nutzernamen anderer Dienste, z.B.
 - aus geleakten Datenbanken
- Generierung von Nutzernamen nach bekanntem Muster
 - viele verwenden Vor- und/oder Nachname als Nutzername
 - fügen am Ende Nummern an, z.B.
 - John64, Robert17, ...
 - Email-Adressen, ...

Erraten von Passwörtern (3/4)

Finden gültiger Passwörter

Um sich Passwörter einfacher zu merken, wählen viele Nutzer einfach strukturierte Passwörter:

- Studien zeigen, dass ca. 10% aller Nutzer ihren Vornamen als Passwort wählen
- Auch werden unveränderte Standardeinstellungen von Nutzer/Passwort Kombinationen (Default) verwendet, mit denen Systeme ausgeliefert werden oder die im Handbuch stehen (Beispiel: private WLAN-Router), z.B.
 - test/test, gast/gast, admin/admin
- Hacker können so einfach Listen mit häufigen Kombination durchprobieren...

Erraten von Passwörtern (4/4)

Verschiedene Studien zur Passwortsicherheit zeigen:

- 20-40% der Passwörter in einer Datenbank können erraten werden
- erste Nutzer/Passwort-Kombination kann meistens schon innerhalb der ersten 15 Minuten gefunden werden
- aktuelle Passwortknacker können pro Minute ca. 1500 Nutzer/Passwort-Kombinationen auf Webseiten testen

Schnelles Erraten wird möglich, weil viele Passwörter trotz Warnung und aus Leichtsinn zu einfach gewählt werden

Knacken von Passwörtern (1/6)

Das sogenannte Knacken von Passwörtern (password cracking) wird offline auf einer Liste von gehashten Passwörtern ausgeführt

Ziel:

- Passwörter im Klartext aus ihren verschleierte Hash-Werten ableiten
- ist oft viel schneller als das Raten von Passwörtern ...

Voraussetzung:

- Zugriff auf eine Nutzerdatenbank mit Passworthashes, z.B.
 - aus geleakter Datenbank oder geknacktem Computer

Knacken von Passwörtern (2/6)

Angreifer versuchen, Passwörter zu knacken entweder mit Hilfe von **Wörterbüchern** oder über **Brute Force** (durch „rohe Gewalt“)

Wörterbuch

- Listen von Wörterbucheinträgen werden nacheinander ghasht
- Hashs werden dann mit vorliegendem Passworthash verglichen

Brute Force

- alle möglichen Zeichenkombinationen werden durchprobiert
- Brute Force Angriffe finden stets das Passwort – dauern aber bei ausreichender Passwortlänge „ewig“ lange (Jahrzehnte, Jahrhunderte, ...)

Knacken von Passwörtern (3/6)

- Programme zum Passwörter-Knacken sind sehr schnell, weil sie sowohl Prozessor(en) als auch Grafikprozessor(en) eines Computer nutzen
- Raten ist immer beschränkt durch Netzwerkbandbreite und anfällig für Störungen und Verzögerungen

Historische Entwicklung:

- vor 40 Jahren konnten drei Passwörter pro Sekunde getestet werden (DEC-PDP-11)
- Heute lassen sich pro Sekunde testen
 - ca. 3 Mrd. SHA1-Passwörter auf aktuellen PC
 - ca. 200 Mrd. MD5-Passwörter auf Clustern aus Grafikprozessoren

Knacken von Passwörtern (4/6)

- Geschwindigkeit beim Passwörter-Knacken ist stark abhängig von verwendeter Hardware: Prozessor (CPU), Grafikprozessor (GPU)
- GPUs sind extrem effizient beim Passwörter-Knacken
 - GPUs sind für parallele mathematische Berechnungen optimiert
 - teils 1.000x schneller als CPUs
- Zeittafel zum Knacken bei 100 Milliarden Tests (mit spezieller Hardware) pro Sekunde:

Password	Time	Password	Time
secret	< 1 Sekunde	secret12	29 Sekunden
!sEcRe!	5,41 Minuten	!secret2	1,45 Stunden
!sEcRe!2	18.62 Stunden	!sEcRe!2%9	19,24 Jahre

Source: <https://www.grc.com/haystack.htm>

Knacken von Passwörtern (5/6)

Es gibt auch freie **Tools zum Passwörter-Knacken** ...

Sehr berühmt und verbreitet:

- **John the Ripper** und **Hashcat**

- beide unterstützen das Knacken der gängigen Passwort-Hash Verfahren, wie z.B. DES, MD5, SHA-1, Blowfish, ...

- **RainbowCrack**

- unterstützt effizientes Knacken mittels vorberechneter Rainbow-Tables
- geeignet nur für Hash-Funktionen ohne Einsatz von Salts

- **L0phtCrack**

- bekannt für effizientes Knacken von Windows-Passwörtern

Knacken von Passwörtern (6/6)

Achtung:

- Gute Passwörter sind nutzlos, wenn eingeschleuste Lauschprogramme jeden Tastenschlag mithören können

Empfehlung:

- Eigene Passwörter gegen frei verfügbare Wortlisten testen, z.B. von
 - <http://www.openwall.com/john/>
 - <http://www.openwall.com/wordlists/>
 - <http://www.oxfordwordlist.com/>
 - <https://www.grc.com/haystack.htm>
 - <https://haveibeenpwned.com/Passwords>

Abfangen von Passwörtern – Sniffing

Weitere Methode zur Erlangung von Nutzernamen und Passwörtern ist Abfangen/Abhören – **Sniffen** –, z.B.

- Belauschen und Analysieren von Netzwerkpaketen in lokalen (LAN) oder kabellosen Netzwerk (WLAN)

Tools:

- Frei verfügbare Werkzeuge: Wireshark, tcpdump, ...

Grundidee:

- Inhalt von (unverschlüsselten) Datenpaketen kann leicht analysiert und gefiltert werden nach Begriffen, wie z.B. „login“ oder „password“

Ausspähen von Passwörtern

Einschleusung/Installation von **Keyloggern**

- Keylogger sind kleine Schadprogramme, die Tastatureingaben aufzeichnen und in spezieller Datei abspeichern
 - für Hacker sind insbesondere Texteingaben im Kontext von „login...“ oder „passw...“ interessant
- Hacker laden Dateien später von System herunter oder lassen sich diese automatisch an ihre zentralen Server (Dropzone) zuschicken und speichern

Zusammenfassung: Angriffe auf Passwörter

Angreifer haben zahlreiche Möglichkeiten entwickelt, um an Passwörter zu gelangen:

- **Erraten** von Passwörtern
- **Knacken** gestohlener Passworthashes
- **Sniffing** – Abfangen von Netzwerkpaketen
- Einsatz von **Software** (Keylogger, Trojaner)
- **Social Engineering Angriffe**