Sichere Passwörter

Warum?

Was nützt die beste Festplattenverschlüsselung wenn ein Angreifer an das Passwort gelangen kann?

Warum?

Was nützt die beste Festplattenverschlüsselung wenn ein Angreifer an das Passwort gelangen kann?
NICHTS!

Passwört-Selbstkontrolle

- sehr schwach: hallo, passwort, deinemutter, 123456
- schwach: Computer123, Lagerfeuer2006
- mittel: (rypto(ON13, LAIB$ig77
- gut: $ubl4bL33!pZig, #7l@gW*tz
- sehr gut: FEl#XU2Ad4@JTCsq6sxyX, QLoD5DDg9VT%GXh7ZPTT

Angriffe gegen Passwörter

- Ausspähen:
  - über die Schulter schauen
  - Filmen
  - mit einem Keylogger
  - Unverschlüsselte Verbindung mitschneiden (z.B. offenes WLAN, Hotspot, ..)

Angriffe gegen Passwörter

- Ausspähen:
  - über die Schulter schauen
  - Filmen
  - mit einem Keylogger
  - Unverschlüsselte Verbindung mitschneiden (z.B. offenes WLAN, Hotspot, ..)
- Erraten:
  - z.B. viel zu einfaches Passwort: hallo, liebe, passwort
  - Wörterbuchattacke, Grammatikanalyse

Angriffe gegen Passwörter

- Ausspähen:
  - über die Schulter schauen
  - Filmen
  - mit einem Keylogger
  - Unverschlüsselte Verbindung mitschneiden (z.B. offenes WLAN, Hotspot, ..)
- Erraten:
  - z.B. viel zu einfaches Passwort: hallo, liebe, passwort
  - Wörterbuchattacke, Grammatikanalyse
- Knacken:
  - Brute-Force-Attacke (alle mgl. Varianten probieren)
  - Hash-Kollisionen (bei unsicheren Hash-Algorithmen)
  - Rainbowtables (bei schlecht gesalteten Passwort-Hashes)

Angriffe gegen Passwörter

- Ausspähen:
  - über die Schulter schauen
  - Filmen
  - mit einem Keylogger
  - Unverschlüsselte Verbindung mitschneiden (z.B. offenes WLAN, Hotspot, ..)
- Erraten:
  - z.B. viel zu einfaches Passwort: hallo, liebe, passwort
  - Wörterbuchattacke, Grammatikanalyse
- Knacken:
  - Brute-Force-Attacke (alle mgl. Varianten probieren)
  - Hash-Kollisionen (bei unsicheren Hash-Algorithmen)
  - Rainbowtables (bei schlecht gesalteten Passwort-Hashes)
- Social Engineering:
  - Vertrauensmissbrauch

Was tun?

- Ausspähen

Was tun?

- Ausspähen
  - Passwörter schnell und verdeckt eingeben

Was tun?

- Erraten

Was tun?

- Erraten
  - Passwort sollte nicht erratbar sein
  - Kein Name von FreundIn, Mutter, Haustier, Notebookhersteller

Was tun?

- Brute-Force-Attacke

Was tun?

- Brute-Force-Attacke
  - Komplexe Passwörter auswählen

Was tun?

- Social Engineering

Was tun?

- Social Engineering
  - **Das Passwort bleibt geheim.**

Was tun?

- Social Engineering
  - **Das Passwort bleibt geheim.**
  - IMMER.

Was tun?

- Social Engineering
  - **Das Passwort bleibt geheim.**
  - IMMER. Ohne Ausnahmen!

Was tun?

- Social Engineering
  - **Das Passwort bleibt geheim.**
  - IMMER. Ohne Ausnahmen!
  - Passwörter nicht leichtfertig eingeben
  - Keinen Links in Emails folgen, die erneute Passworteingabe fordern (Phishing)
  -

Brute Force Attacken

- Nacheinander Durchprobieren aller mgl. Kombinationen

Brute Force Attacken

- Nacheinander Durchprobieren aller mgl. Kombinationen
- Benutzung von Wortlisten (Wörterbuchattacke)
- Grammatikanalyse (Kombination aus Wörtern die Sätze bilden)

Brute Force Attacken

- K - Kleinschreibung
- G - Grossschreibung
- Z - Zahlen
- S - Sonderzeichen

L	K
1	26
2	676
4	4.569.768
8	208.827.064.576

Brute Force Attacken

- K - Kleinschreibung
- G - Grossschreibung
- Z - Zahlen
- S - Sonderzeichen

L	K+G
1	52
2	2704
4	7.311.616
8	53.459.728.531.456

Brute Force Attacken

- K - Kleinschreibung
- G - Grossschreibung
- Z - Zahlen
- S - Sonderzeichen

L	K+G+Z
1	62
2	3844
4	14.776.336
8	218.340.105.584.896

Brute Force Attacken

- K - Kleinschreibung
- G - Grossschreibung
- Z - Zahlen
- S - Sonderzeichen

L	K+G+Z+S
1	92
2	8464
4	71.639.296
8	5.132.188.731.375.616

Brute Force Attacken

- Angreifer: probiert 1.000.000 Passwörter pro Sekunde

Brute Force Attacken

- Angreifer: probiert 1.000.000 Passwörter pro Sekunde
- Angreifer benötigt dann im Worst Case:

Brute Force Attacken

- Angreifer: probiert 1.000.000 Passwörter pro Sekunde
- Angreifer benötigt dann im Worst Case:
- Passwort mit Kleinschreibung, 8 Zeichen:
  58 Stunden (ca. 2,5 Tage)

Brute Force Attacken

- Angreifer: probiert 1.000.000 Passwörter pro Sekunde
- Angreifer benötigt dann im Worst Case:
- Passwort mit Kleinschreibung, 8 Zeichen:
  58 Stunden (ca. 2,5 Tage)
- Passwort mit Gross- u. Kleinschreibung, Zahlen und Sonderzeichen, 8 Zeichen:
  mehr als 60.000 Stunden (ca. 7 Jahre)

Ein sicheres Passwort wählen

Ein sicheres Passwort ...
... ist mindestens 8 Zeichen lang

Ein sicheres Passwort wählen

Ein sicheres Passwort ...

... ist mindestens 8 Zeichen lang

... beinhalteltet Groß- und Kleinschreibung

Ein sicheres Passwort wählen

Ein sicheres Passwort ...

... ist mindestens 8 Zeichen lang

... beinhalteltet Groß- und Kleinschreibung

... besteht auch aus Zahlen und Sonderzeichen

Ein sicheres Passwort wählen

Ein sicheres Passwort ...

... ist mindestens 8 Zeichen lang

... beinhalteltet Groß- und Kleinschreibung

... besteht auch aus Zahlen und Sonderzeichen

... missachtet, sofern es ein Satz ist, korrekte Grammatik

Ein sicheres Passwort wählen

Beispiel:

- Schritt 1 - Länge:

atomkraftwerk

Ein sicheres Passwort wählen

Beispiel:

- Schritt 1 - Länge:

  atomkraftwerk

- Schritt 2 - Grammatik:

  atomwerkkraft

Ein sicheres Passwort wählen

Beispiel:

- Schritt 1 - Länge:

  atomkraftwerk

- Schritt 2 - Grammatik:

  atomwerkkraft

- Schritt 3 - Groß- und Kleinschreibung:

  atoMWerkkrAFT

Ein sicheres Passwort wählen

Beispiel:

- Schritt 1 - Länge:

  atomkraftwerk

- Schritt 2 - Grammatik:

  atomwerkkraft

- Schritt 3 - Groß- und Kleinschreibung:

  atoMWerkkrAFT

- Schritt 4 - Zahlen:

  atoM5Werkkr4FT

Ein sicheres Passwort wählen

Beispiel:

- Schritt 1 - Länge:

  atomkraftwerk

- Schritt 2 - Grammatik:

  atomwerkkraft

- Schritt 3 - Groß- und Kleinschreibung:

  atoMWerkkrAFT

- Schritt 4 - Zahlen:

  atoM5Werkkr4FT

- Schritt 5 - Sonderzeichen:

  a-toM5%Werkkr4FT

Ist es auch sicher?

Beispiel:

- 16 Stellen, Gross- und Kleinschreibung, Zahlen und Sonderzeichen

Ist es auch sicher?

Beispiel:

- 16 Stellen, Gross- und Kleinschreibung, Zahlen und Sonderzeichen
- Ich habe einen Superrechner und probiere 1 Billion Passwörter pro Sekunden (1.000.000.000.000)

Ist es auch sicher?

Beispiel:

- 16 Stellen, Gross- und Kleinschreibung, Zahlen und Sonderzeichen
- Ich habe einen Superrechner und probiere 1 Billion Passwörter pro Sekunden (1.000.000.000.000)
- Dann bin ich die nächsten 834.646.274.998 Jahre beschäftigt

Best Practices

- Sichere Passwörter wählen
- Passwörter sollten regelmässig geändert werden
- Ein Passwort pro Service
- Vor Eingabe: auf verschlüsselte Verbindungen achten
- Passwörter nur auf vertrauenswürdigen Systemen eingeben
- Passwörter nicht unverschlüsselt notieren
- Passwörter sichern (Backup, auch Offsite)

Passwörter verwalten

- Merken

Passwörter verwalten

- Merken
- Passwort-Manager

Passwörter verwalten

- Merken
- Passwort-Manager
  - speichern alle Passwörter verschlüsselt in Datenbank
  - ein Masterpasswort
  - Einzelanwendung
    z.B. KeepassX (Linux)
  - Browser-Plugin
    z.B. LastPass (Firefox)

Sicherheitsfragen

- Typische Fragen:
  - Mädchenname der Mutter

Sicherheitsfragen

- Typische Fragen:
  - Mädchenname der Mutter
  - Name des Haustieres

Sicherheitsfragen

- Typische Fragen:
  - Mädchenname der Mutter
  - Name des Haustieres
  - Name der Patentante

Sicherheitsfragen

- Typische Fragen:
  - Mädchenname der Mutter
  - Name des Haustieres
  - Name der Patentante
- potentielles Sicherheitsrisiko

Sicherheitsfragen

- Warum?
- Alle Informationen lassen sich erraten oder erfragen (Social Engineering)

Sicherheitsfragen

- Was tun?
- Felder mit Zufallspasswort füllen
- z.B. Mädchenname der Mutter: QLoD5DDg9VT%GXh7ZPTT
- Passwort-Manager zur Verwaltung benutzen

Passwörter für Cryptocontainer

Passwörter für Cryptocontainer (z.B. verschlüsselte Festplatten) sollten besonders schwer zu knacken sein

Passwörter für Cryptocontainer

Passwörter für Cryptocontainer (z.B. verschlüsselte Festplatten) sollten besonders schwer zu knacken sein
Anforderungen:

- vielfältig

Passwörter für Cryptocontainer

Passwörter für Cryptocontainer (z.B. verschlüsselte Festplatten) sollten besonders schwer zu knacken sein
Anforderungen:

- vielfältig
- geheim
- nur einmalig verwendet

Passwort Backup

- Passwörter nicht im Klartext notieren

Passwort Backup

- Passwörter nicht im Klartext notieren
- Passwortdatenbank sichern.

Passwort Backup

- Passwörter nicht im Klartext notieren
- Passwortdatenbank sichern. Mehrfach.
- z.B. auf (verschlüsselten) Festplatte

Quellen

- Grundlegendes:
  http://www.uni-due.de/zim/services/sicherheit/sicheres_passwort.shtml
- Grammatikanalyse:
  http://www.pressetext.com/news/20130126003

Online

http://cryptocrew.eu