Passwörter

Warum sind Passwörter wichtig?

Eine Verschlüsselung ist nur so sicher
wie das verwendete Passwort

Oft das schwächste Glied in der Kette

Wenig Aufwand ermöglicht sichere Passwörter

Was macht ein Passwort sicher?

Durchschnittliche Zeit die
ein Angreifer zum Raten benötigt

Messbar in Bits:
jedes weiter Bit $\longrightarrow$ Verdoppelung des Zeitaufwands

Ein zufälliges Wort: ca. 11 Bits

Zufällige Kleinbuchstaben: 4.7 Bit/Zeichen

Kleinbuchstaben & Zahlen: 5.2 Bit/Zeichen

Klein., Groß., Zahlen & Sonderzeichen: 6.4 Bit/Zeichen

Wie sicher muss ein Passwort sein?

Abhängig von der Verwendung

Minimum: ca. 60 Bits
6 zufällige Wörter oder 10 bis 12 Zeichen
Längst nicht in jedem Fall sicher!

Physikalisch unknackbar: 120 Bits
12 zufällige Wörter oder 20 bis 24 Zeichen

Passworthygiene

Keine Passwörter doppelt verwenden

E-Mail Passwörter nicht bei
sozialen Netzen angeben

Passwörter nicht an Dritte weitergeben

Bei Bekanntwerden von
Sicherheitslücken Passwörter wechseln

Passworthygiene

Sich nicht beim Eingeben über
die Schulter schauen lassen

Passwörter nicht unverschlüsselt übermitteln
(auf https:// achten, SSL oder TLS
bei E-Mail Programmen)

Passwörter nicht unverschlüsselt aufschreiben

Passwordmanager

Sichere Verwendung von Passwörtern ist schwer und umständlich

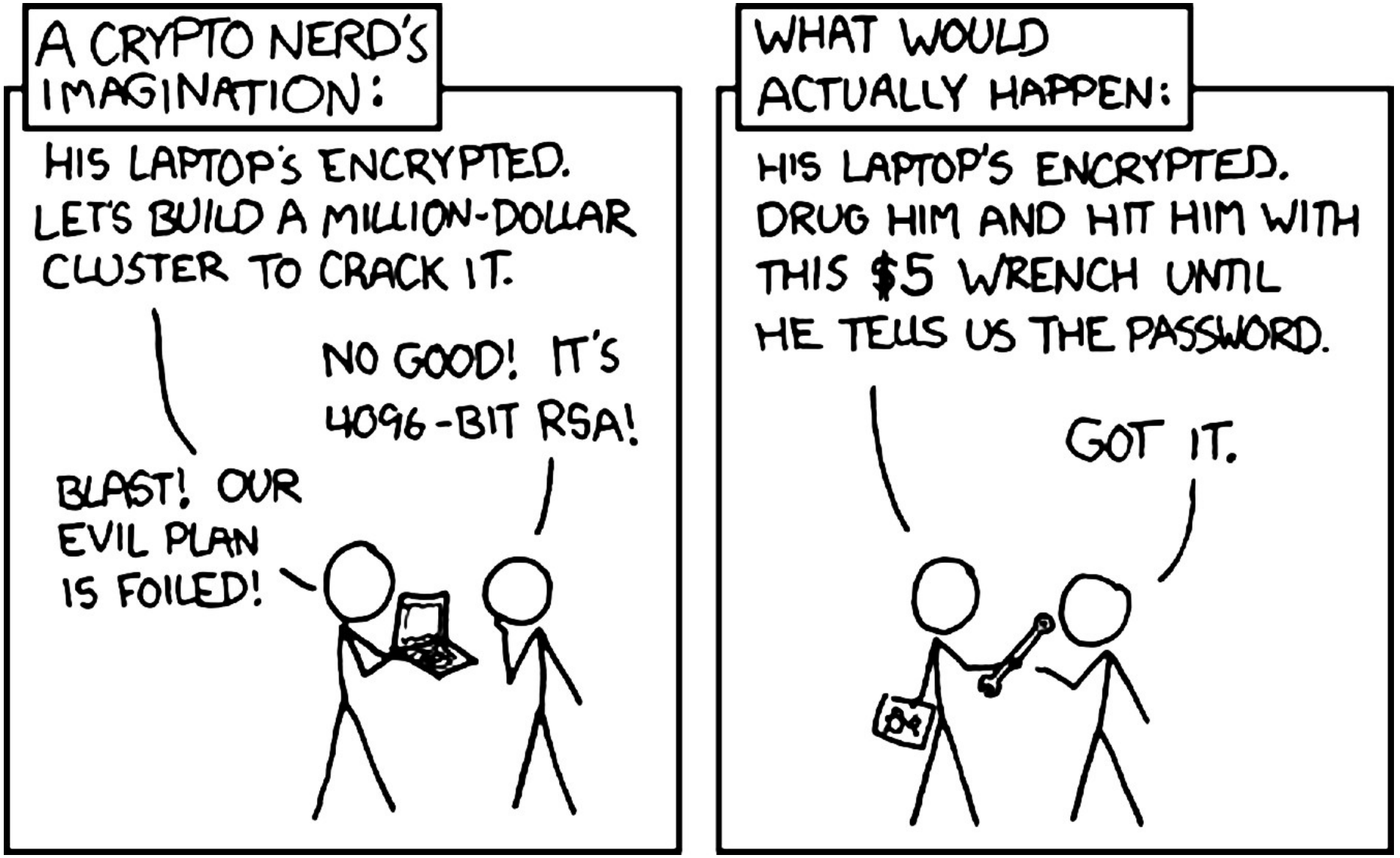
Passwordmanager helfen hier

Passwörter werden zufällig und in ausreichender Länge generiert

Passwörter werden sicher mit einem Masterpassword gespeichert

Passwordmanager in der Praxis

Grenzen der Verschlüsselung



Quelle: http://xkcd.com/538/

Grenzen der Verschlüsselung

Verschlüsselung schützt Nachrichten
bei der Übertragung

Z.B. vor massenhafter Überwachung

Jedoch nicht der einzige Angriffspunkt

Angriffe auf die Software

Spy- & Malware: Toolbars, Programme aus fragwürdigen Quellen

Viren & Würmer

Hintertüren von Herstellern & Anbietern

Computer können auch gezielt angegriffen werden

Freie Software bzw. Open Source Software
bietet hier viele Vorteile

Angriffe auf den Nutzer

Klassische Überwachung

Gesetze die das Herausgeben
von Passwörtern vorschreiben

Manipulation von Computern und
Netzwerkequipment