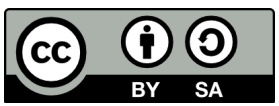
Cryptoparty

Florian Wilde

basierend auf „Cryptoparty an der LMU“ von Michael Weiner

26. Oktober 2015



Fahrplan

Über den Veranstalter und Cryptopartys

Grundlegendes

Passwörter

Web-Surfen

E-Mail

Fragen, Feedback

Fahrplan

Die Veranstalter

- Chaos Computer Club München e.V.
- Forum InformatikerInnen für Frieden
  und gesellschaftliche Verantwortung e.V.
- Medienzentrum München (MZM)
  Institut für Medienpädagogik in Forschung und Praxis
  JFF – Jugend Film Fernsehen e.V.

Die Cryptoparty

- Weltweite Bewegung von technisch interessierten
- Ziel: Datensicherheit für jedermann
- Themen sind z.B.
  - Kommunikation: E-Mail, Anrufe, Chat
  - Datenspeicherung und -weitergabe
  - Veröffentlichen von Informationen
  - Passwörter
- Aus Zeitgründen beschränken wir uns heute auf
  - Passwort-Management
  - Anonyme(re)s Web-Surfen
  - E-Mail-Verschlüsselung und -Signatur
  - . . . und mehr auf Anfrage, wenn noch Zeit ist

Fahrplan

Warnhinweise

- 100% Sicherheit gibt es nicht
- Absichern heißt, Angriffe *teurer* zu machen
  - Die Kosten für den Angriff müssen den Wert der Daten übersteigen
  - Ein Angriff darf sich nicht mehr *lohnen*
  - Problem: Wert wird oft unterschätzt
- Was wir hier zeigen, ist ein Anfang
  - Hilft dagegen, als „Beifang“ zu enden
  - Gegen gezielte Angriffe – auch durch Verwechslung – benötigt es deutlich mehr

Leitfragen

- *Was* soll sichergestellt werden?
  - Eigene Anonymität
  - Echtheit des Gegenübers (Authentizität)
  - Unverfälschtheit der Nachricht (Integrität)
  - Geheimhaltung der Nachricht (Vertraulichkeit)
  - ...
- *Wem* vertraut Ihr?

Vertrauen

Woher weiß man, wem man vertrauen kann?

- Kurze Antwort: weiß man *nicht*
- Lange Antwort
  - es gibt Fragen, die man stellen kann. . .
  - . . . und es gibt das Bauchgefühl

Welche Fragen kann man stellen?

Beispiel: *Wo* sind meine Daten?

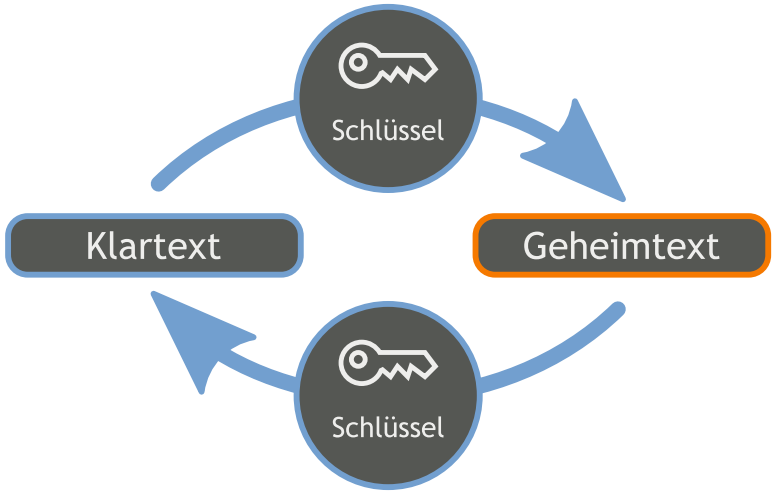
- Auf einem Blatt Papier zuhause in meiner Schublade.
- Auf meinem Computer:
  - Wie gut ist die Software *überprüfbar*, die meine Daten verwaltet?
    - Open Source (in menschenlesbarer Form öffentlich): gut überprüfbar
    - Closed Source (menschenlesbare Form geheim): quasi nicht überprüfbar
- In der Cloud
  - *Wer* betreibt einen Dienst?
  - Womit *verdient* der Betreiber sein *Geld*?
  - Wem könnten die Daten *Nutzen* oder *Schaden*?
  - *Welche zusätzliche Daten* fallen beim Betreiber an?

Meta- und Nutzdaten

- Meta-/Verbindungsdaten (“Briefumschlag”)
  - Absender, Empfänger, Betreff einer E-Mail
  - Besuch und Aufenthaltsdauer auf einer Webseite
  - Wer, wann, wie lange mit wem telefoniert
  - Aufenthaltsort von Mobiltelefonen: Bewegungsprofil!
- Nutz-/Inhaltsdaten (“Brief”)
  - E-Mail-Text und -Anhänge
  - Webseiten-Inhalte
  - Gesprochene Sprache beim Telefonieren
  - SMS-Inhalt

Metadaten zu verschlüsseln ist nicht möglich,
sie zu verschleiern schwierig.

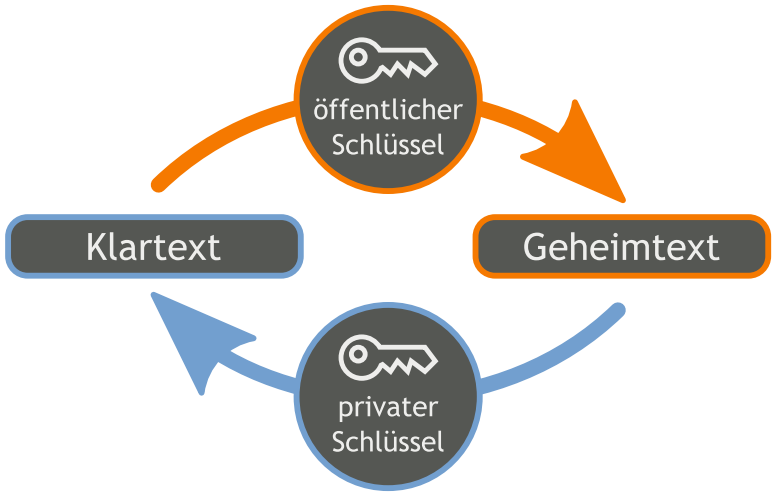
Symmetrische Kryptographie



- Jahrtausende altes Konzept
- *Ein* Schlüssel zum Ver- und Entschlüsseln, den *alle* Beteiligten kennen
- Problem: Schlüsselaustausch
  - Wer den Schlüssel kennt, kommt auch an die Daten
  - Wer den Schlüssel manipuliert, kontrolliert die Daten
- Wird überall verwendet, um Inhalte zu verschlüsseln

Bildquelle: `https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem`

Asymmetrische Kryptographie



- Prinzip: Schlüssel besteht aus einer *privaten* und einer *öffentlichen* „Hälfte“
  - Öffentlichen Teil darf/muss man weitergeben
  - Privaten Teil muss man unbedingt geheim halten
- Wird verwendet, um vertraulichen Kanal aufzubauen
- Problem weiterhin: Authentizität des öffentlichen Teils

Bildquelle: `https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem`

Asymmetrische Kryptografie – Anwendungen

- Verschlüsselung
  - Absender *verschlüsselt*
    mit *öffentlichem* Teil des *Gegenübers*
  - Nur Gegenüber
    kann mit *privatem* Gegenstück *entschlüsseln*
- Digitale Signatur
  - Absender unterschreibt mit *eigenem privaten* Teil
  - Jeder kann mit *öffentlichem* Gegenstück *überprüfen*

Es ist mathematisch komplex und benötigt Jahrtausende, um aus einer Signatur oder dem öffentlichen Teil den privaten Teil zu berechnen

Fahrplan

Passwörter

Wer hat mindestens fünf Online-Accounts?

Passwörter

Wer hat mindestens fünf Online-Accounts?
Wer hat dafür mindestens drei verschiedene Passwörter?

Passwörter

Wer hat mindestens fünf Online-Accounts?
Wer hat dafür mindestens drei verschiedene Passwörter?
Wer beachtet, Passwörter nur über HTTPS einzugeben?

Anzahl Passwörter

- Kundendaten gehen häufig verloren
  - Schaden lässt sich begrenzen, wenn Benutzername und Passwort nur bei diesem einen Anbieter passen
- Besonder wichtig: E-Mail Accounts
  - Weil „Passwort zurücksetzen“ oft via E-Mail
  - Wer den E-Mail Account übernommen hat, kann dadurch sämtliche Accounts übernehmen
- Ideal: Jedes Passwort nur einmal verwenden
- Alternative: Passwörter „salzen“
  - *passwort*.amz für Onlineshop a
  - *passwort*.zal für Onlineshop z
  - *anderespasswort* für Mails

Sichere Passwörter

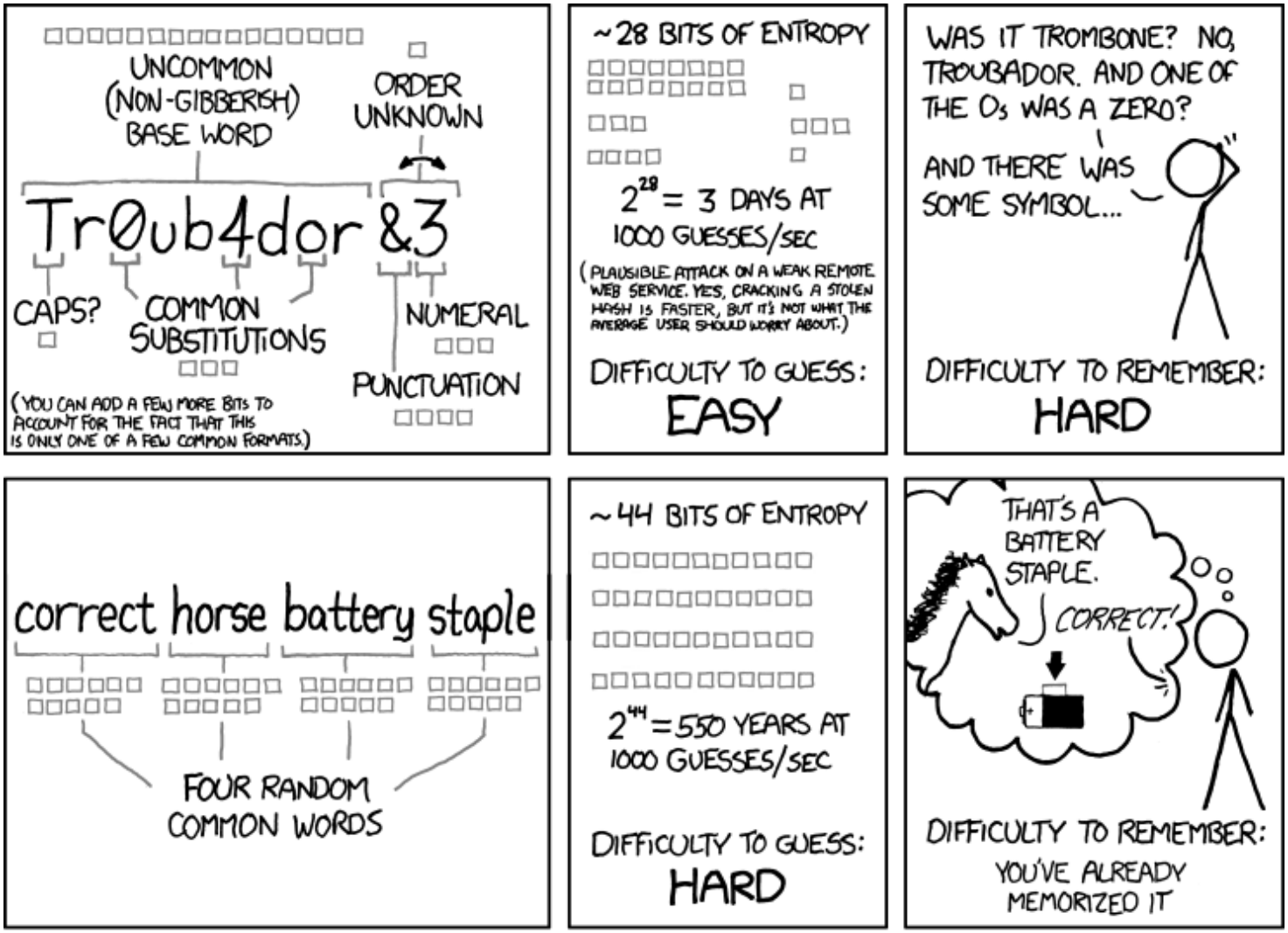
Anforderungen

- Klein- und Großbuchstaben, Zahlen, begrenzt: Sonderzeichen
- Wichtiger: Lang genug!

Merkbarkeit

- Geschichte dazu ausdenken
- Melodie und Rhythmus rein bringen
  - Gehirn kann sich Melodien besonders leicht merken
  - Ermöglicht schnelles eintippen
    - Längere Passwörter sind weniger nervig
    - Passwort mitlesen ist schwieriger

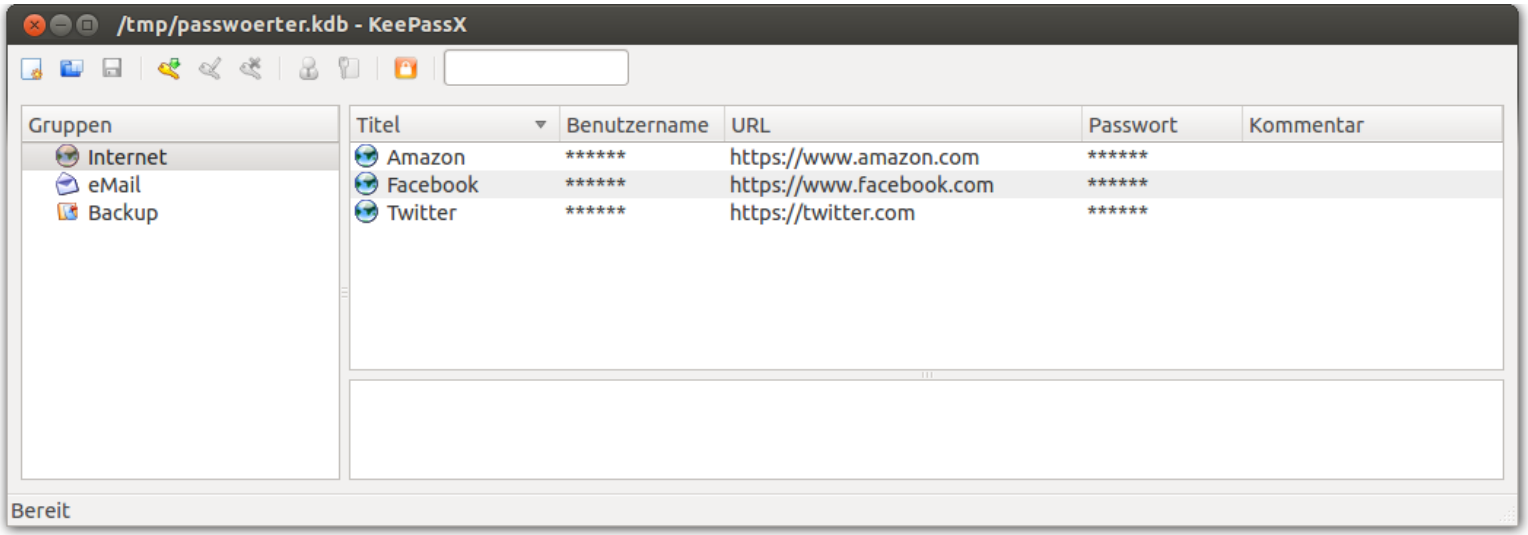
Passwort Länge vs. Zeichensatz



Quelle: `http://xkcd.com/936/`

Passwort-Manager

- Software zur Verwaltung von Passwörtern
- Kann automatisch komplexe Passwörter erzeugen
- Datenbank wird mit Master-Passwort verschlüsselt
  - Anzahl der zu merkenden Passwörter geringer
- Beispiel: KeePassX (Open Source)



- *Wichtige Passwörter trotzdem merken!*
- . . . oder zumindest auf einem Zettel aufschreiben und zuhause an einem sicheren Ort lagern

Fahrplan

Problem: Trackbarkeit

- Cookies und Co (HTML5 Persistent Local Storage, Flashcookies, . . .)
- Browser-Fingerabdruck
- IP-Adresse

Nicht nur die NSA, auch jede Website
und jeder Werbeanbieter kann einen (wieder-)erkennen

Tools zur Aufklärung

- EFF: Panopticlick
- Wired: Datenblumen

Schutzmaßnahmen – Level 1

Nur Einstellungen ändern

- Standardsuchmaschine
  auf datenschutzfreundliche Anbieter ändern, z.B.
  - DuckDuckGo
  - Startpage
  - ixquick
- Cookies verbieten, nur selektiv erlauben
  - Firefox: about:preferences
- Add-Ons auf „Click-to-use“ stellen
  - Firefox: about:addons

Eventuell:

- Blockierung von „bösen“ Webseiten abschalten
- Statusberichte des Browsers abschalten

Schutzmaßnahmen – Level 2

Plug-Ins installieren

- Adblocker –
  Schadsoftware immer öfter über Werbeanzeigen!
  - Adblock Edge = Adblock Plus ohne „acceptable Ads“
- NoScript
  - Erlaubt gezieltes ein-/ausschalten von Java, JavaScript etc.
- EFF: HTTPS-Everywhere
  - Nutzt automatisch HTTPS, falls von Seite unterstützt
  - Benutzt lokale Liste der Seiten, keine Online-Abfrage
- RefControl
  - HTTP-Referrer = von welcher Seite komme ich

Schutzmaßnahmen – Level 3

Neue Programme installieren oder benutzen

- TOR Browser Bundle (Open Source)
  - Mehrere Verschlüsselungsschichten,
    wie in einer Zwiebel (TOR = The Onion Router)
  - Datenstrom fließt über mehrere „Bridges“,
    jede kennt nur den Schlüssel für ihre Schicht
  - Fingerabdruck bei allen TOR Browsern identisch
  - Hohe Sicherheit, aber Prinzip bedingt langsamer
- Tails (OpenSource)
  - Abgesichertes Betriebssystem inkl. TOR
  - Schützt vor Schadsoftware,
    die aus dem Browser ausbricht
  - Live System = kann direkt von CD gebootet werden
    hinterlässt keinerlei Spuren am PC
  - Sieht auf Wunsch nach Windows aus

Fahrplan

E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man

- die Vertraulichkeit (das „Briefgeheimnis“) umsetzt
  $\Rightarrow$ Verschlüsselung
- die Echtheit des Gegenübers sicherstellt
  $\Rightarrow$ Digitale Signatur

Außerdem:

- Wie man sicherstellt, dass sein E-Mail Passwort nicht einfach mitgelesen werden kann

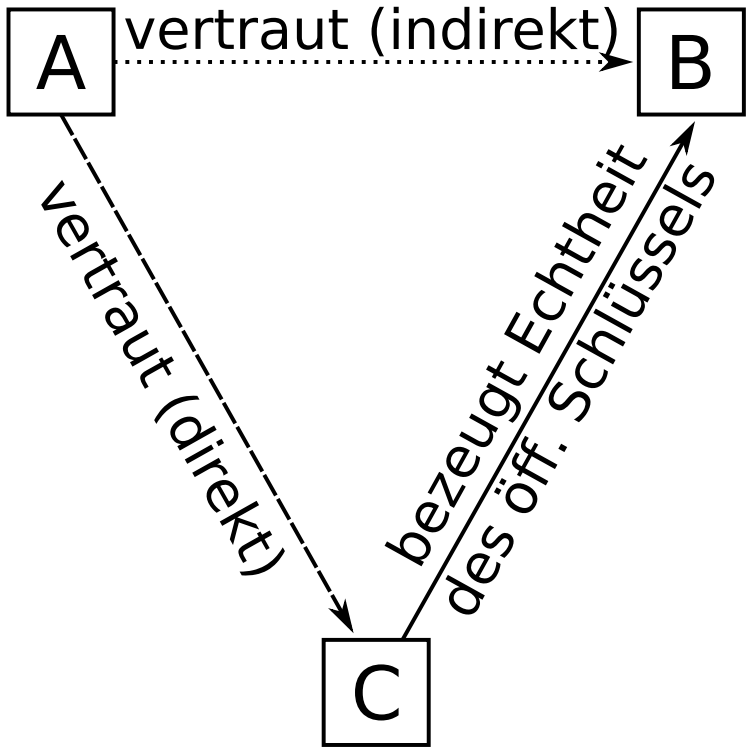
Analogie zur Vertraulichkeit von E-Mails

- E-Mails sind „Postkarten“
- Transportiert in „gläsernen Fahrzeugen“
  - „Autobahnbetreiber“ kann alles mithören
  - „Post“ kann alles mithören
- Bei *Transportverschlüsselung* ersetzt die „Post“ „gläserne Fahrzeuge“ durch „blickdichte Fahrzeuge“
  - „Autobahnbetreiber“ kann mithören,
    wann welche „Post“ mit welcher „Post“ redet
    aber nicht Passwort, Empfänger, Betreff, etc.
  - „Post“ kann alles mithören
- Bei *Ende-zu-Ende-Verschlüsselung* steckt der Absender die „Postkarte“ in einen „Briefumschlag“
  - „Autobahnbetreiber“ und „Post“ können mithören,
    wann wer mit wem wie viel kommuniziert
    aber nicht den Inhalt!
- Unbedingt beides kombinieren!

Überprüfung der Echtheit

Was, wenn A eine Nachricht an B schicken will,
aber den öffentlichen Schlüssel von B nicht kennt?

1. Im “Telefonbuch” nach dem Schlüssel suchen
2. Echtheit mit Hilfe eines *vertrauenswürdigen Dritten* C überprüfen



Wie stellt man Vertrauen her?

- S/MIME – Hierarchischer Vertrauensansatz
  - Es gibt „zentrale Vertrauensinstanzen“ (Certification Authorities, CAs), denen *jeder* vertraut
  - Diese bestätigen die Echtheit der Schlüssel von untergeordneten CAs
  - Eine beliebige CA aus der Vertrauenskette kann einer Person einen Schlüssel zuordnen
  - wird hier *nicht* behandelt
- GnuPG – Dezentraler Vertrauensansatz
  - jeder kann festlegen, wem er vertraut
    - er kann die Echtheit eines Schlüssels z.B. bei einem persönlichen Treffen überprüfen
  - jeder *kann* sein Vertrauensnetz veröffentlichen (Web-of-Trust)
    - Vorteil: Man kann “Freunden von Freunden” vertrauen
    - Nachteil: Beziehungen zwischen Menschen öffentlich Aber: Facebook sagt da viel mehr aus
  - wird hier behandelt

Fahrplan

Über den Veranstalter und Cryptopartys

Grundlegendes

Passwörter

Web-Surfen

E-Mail

Fragen, Feedback

Fragen, Feedback, ...

- Her damit!
- Fragen an alle Helfer (bitte gebt Euch zu erkennen :-)
- Links: `https://muc.pads.ccc.de/cryptoparty`