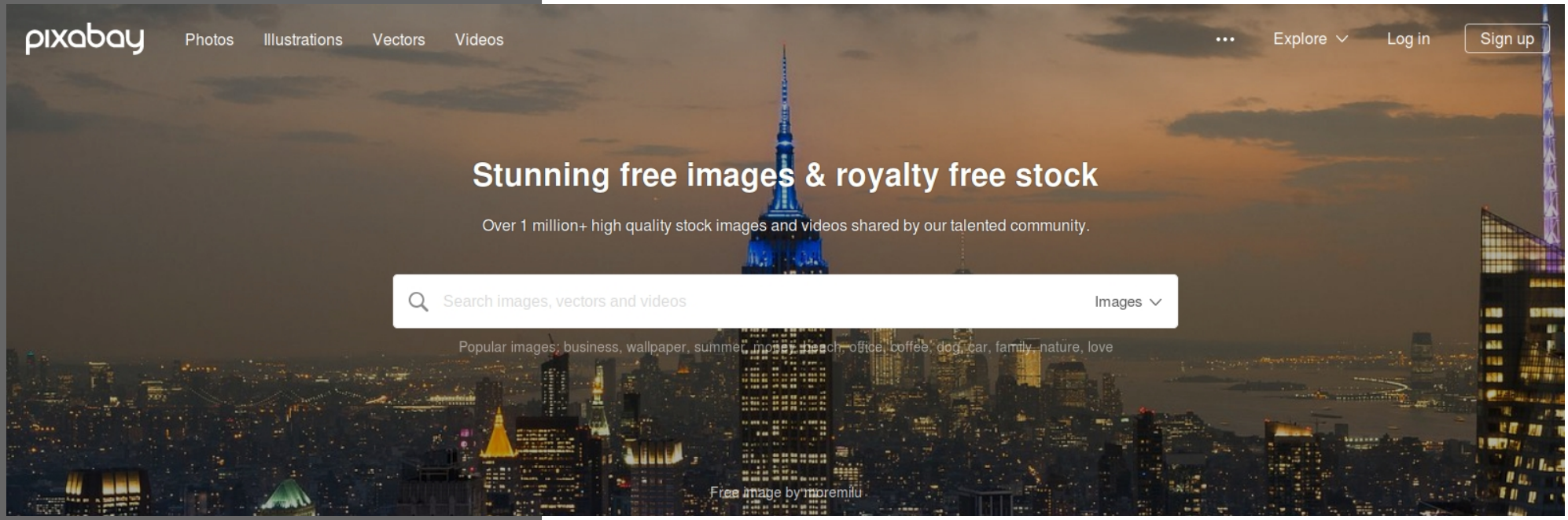
Cryptoparty – Tübingen 27.07.2019

Passwortmanagement

Teaser

Bilder von: **pixabay.com:**

- kostenlose Bilder
- ohne Bildnachweis




Frequently
asked
Questions

Agenda

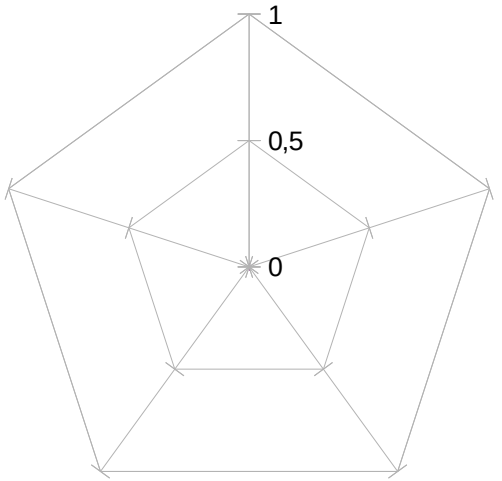
- ✔ Motivation
- ✔ Kontrolle
- ✔ Verwaltung
- ✔ Ausblick

Warum?

Wofür?

Anwendbarkeit

Für welche Anwendungsfälle ist das Passwort „sinnvoll“ (Forum, Onlinebanking, E-Mail, ...)



Variabilität

Wie leicht kann das Passwort an unterschiedliche Passwortrichtlinien angepasst werden.

Sicherheit

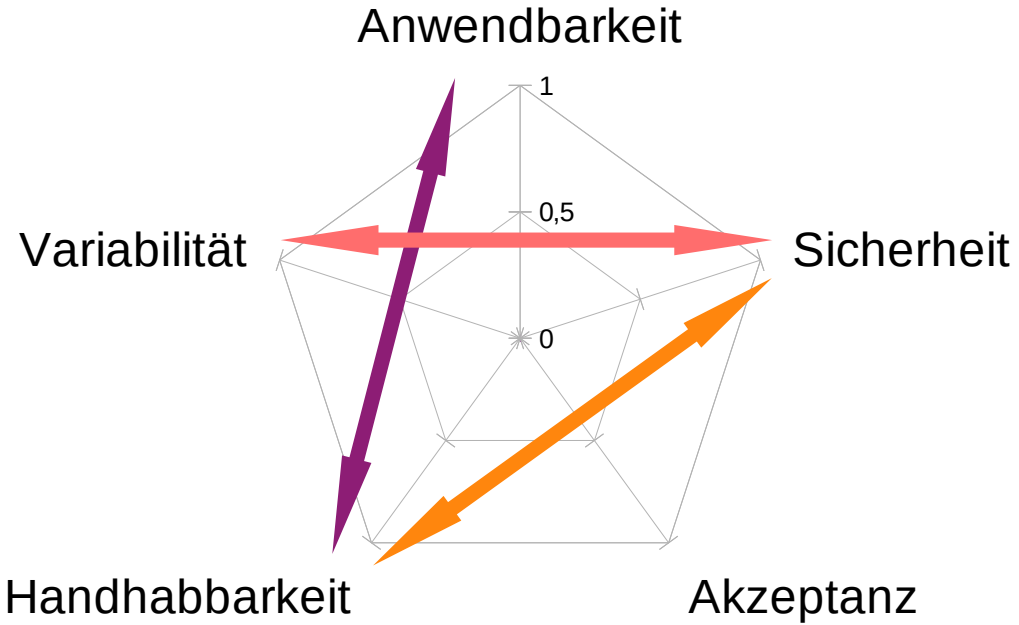
Handhabbarkeit

Wie gut können viele Verschiedene Passwörter von mir gehanhabt werden?

Akzeptanz

Wieviele unterschiedliche Passwortrichtlinien werden hiermit erfüllt?

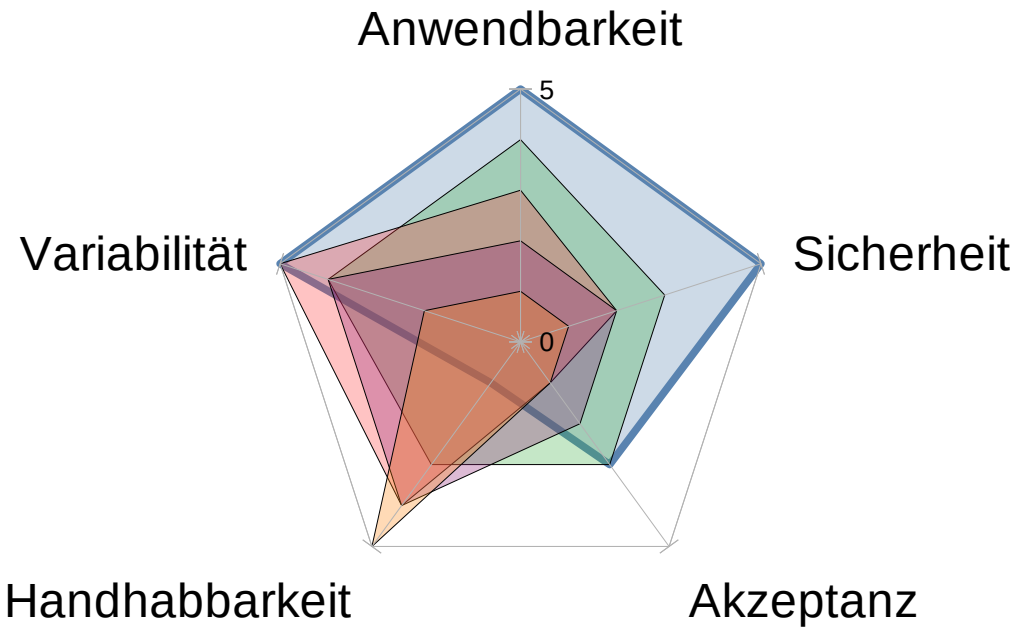
Komplexität



Kategorien zur Reduktion der Komplexität?

- Kritisch
- Wichtig
- Normal
- Unwichtig

Passwort-vergleich



Mama

27.07.2019

IchWohneInTübingen

SauerkrautStabilisiertKartenhäuser

23ffa(43wf9/ w3cbnk“+987l@ös93ay%!

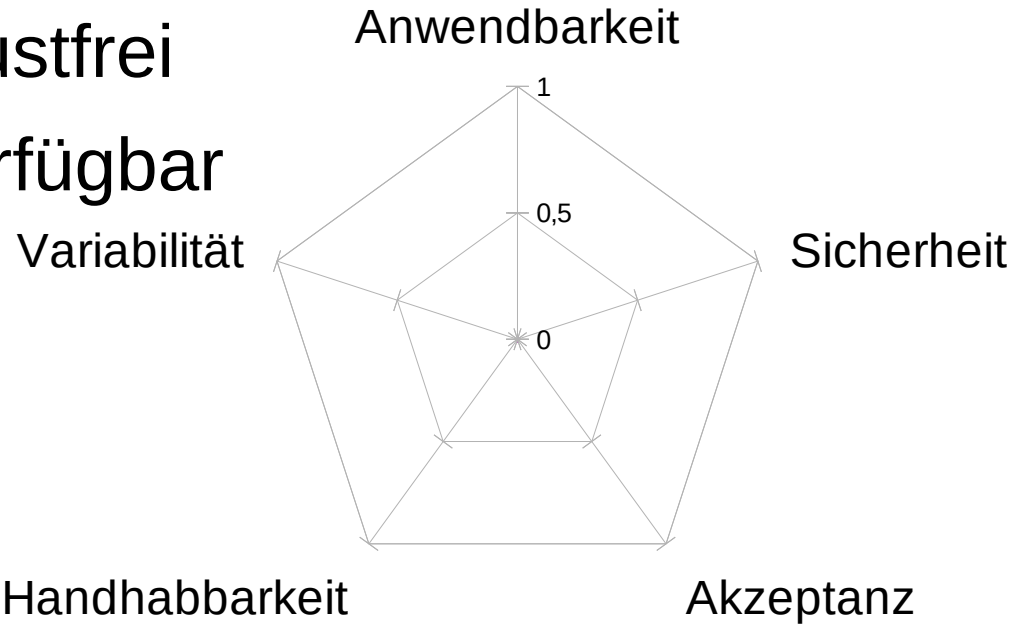
Zusammenfassung

Was ist das wichtigste Kriterium?

H

Kategorien

- Kriterien für einen hohen Happiness-Faktor
  - Usability
  - Pragmatisch
  - Frustfrei
  - Verfügbar



Komplexität

- Wie komplex sollte ein Passwort sein?
  - Angemessen zum Einsatzzweck
  - Angemessen bzgl. des Risikos
  - Angemessen zur nötigen Verfügbarkeit

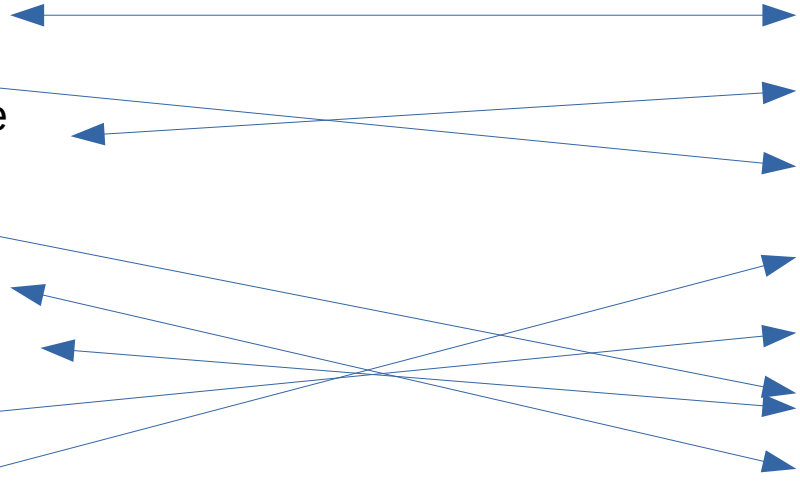
- Analogie
  - Haustürschlüssel ↔ Zimmertür
  - Autoschlüssel ↔ Fahrradschloss
  - Tresor ↔ Tagebuch
- Beispiele
  - Bankzugänge: Möglichst unterschiedlich, sehr komplex
  - Shops: Unterschiedlich, komplex
  - E-Mail-Zugänge: Unterschiedlich, komplex bis sehr komplex
  - Foren, Webservices, Nutzeraccounts, Handy, …

Kategorien

Achtung, Analogie!

Reduktion der Komplexität

- Kategorien bilden
  - Bankzugänge
  - Shops
  - E-Mail-Zugänge
  - Foren
  - Webservices
  - Nutzeraccounts
  - Handy
  - EC-Karte
  - …



- Prioritäten definieren
  - Todernst
  - Essentiell, fast
  - Es gibt kaum wichtigeres
  - Sehr wichtig
  - Wichtig
  - Och ja
  - Egal
  - …

Kategorien helfen, wichtige Bereiche zu schützen, allerdings auf Kosten der Sicherheit anderer Bereiche


Warning!!
18 +

Komplexität

=
Anzahl der theoretisch verfügbaren Zeichen
^
Länge der Zeichenfolge

- Kombinatorik:
  - Anzahl möglicher Kombinationen
    Beispiel: Ziffern 0 bis 9
    - Länge 1:

      10 Kombinationen (10 * 1 = 10^1)
    - Länge 2:

      100 Kombinationen (10 * 10 =10^2)
    - Länge 3:

      1000 Kombinationen (10 * 10 * 10 = 10^3)

Komplexität

# Zeichen	Länge	Anzahl Kombinationen	Bsp.
2	4	16	1101
3	4	81	abca, bbcb
4	4	256	abcd, abbc
62	4	14.776.336	j28d
62	8	218.340.105.584.896	t9MxW4kP
62	12	3.226.266.762.397.899.821.056	ldmePad12Zli

~ 3 Mrd * 100 Mrd
= recht große Zahl

(3*10^9 * 10^12)
= 3*(10^21)
= 3. 000.000.000. 000.000.000. 000

Komplexität

Annahme: 1 Vergleich = 1 Rechenoperation

- Samsung Galaxy S7: 8 Kerne, 2.3 Ghz

  ca. 8 * 2.3 * 10^9 Vergleiche pro Sek
- Apple Iphone 7: 4 Kerne, 2.3 GHz

  ca. 4 * 2.3 * 10^9 Vergleiche pro Sek

PW	Anzahl Kombinationen	Dauer Galaxy S7	Dauer Iphone 8
1101	16	<< 1 Sek	<< 1 Sek
abca, bbcb	81	<< 1 Sek	<< 1 Sek
abcd, abbc	256	<< 1 Sek	<< 1 Sek
j28d	14.776.336	<< 1 Sek	<< 1 Sek
t9MxW4kP	218.340.105.584.896	~ 12.000 Sek (~200min)	~ 24.000 Sek (~400min)
IdmePad12Zli	3.226.266.762.397.899.821.056	~ 49 Mio h (5,5 Jahre)	96,5 Mio h (~11 Jahre)

Begriffs-klärung

	Länge	Verfügbare Zeichen	Bemerkungen
PIN	kurz	Meist nur Ziffern	Wenige Wiederholungen, online
Passwort	Human-Readable	Beliebige Zeichenkette (meist ausgewählte Sonderzeichen)	Online: begrenzte ... Offline: beliebige ... … Anzahl Wiederholungen
Schlüssel / Key	Quasi beliebige Länge	Beliebige Zeichenkette	Gesichert durch Passwort,
Zertifikat	Quasi beliebige Länge	Beliebige Zeichenkette	Gesichert durch Passwort
Hash(-wert)	Konfigurierbare Länge	Beliebige Zeichenkette	Berechnete, scheinbar zufällige Zeichenfolge

Begriffs-klärung

	Beispiel für Verwendung
PIN	Handy, SIM-Karte (PUK), EC- / Kreditkarte, Türschlösser, ...
Passwort	Accounts von E-Mail, Betriebssystem, Foren, … , „öffnen von Schlüsseln, Zertifikaten“, ...
Schlüssel / Key	E-Mail-Verschlüsselung, Zugriffsrechte, Authentifizierungssysteme
Zertifikat	Netzwerktraffic, Zugangssysteme, Authentifizierungssysteme
Hash (-wert)	Verschleiern der originalen Zeichenketten

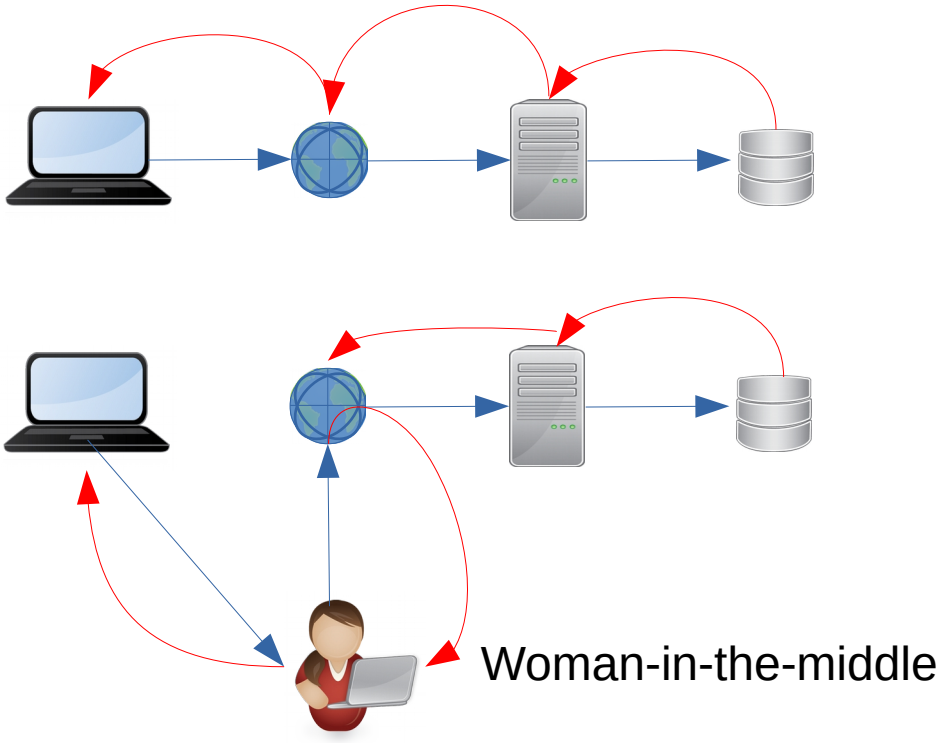
Angriffe

- Online-Angriffe:
  - Angriffe während der Authentifizierung
- Offline-Angriffe
  - Angriffe, basierend auf „erworbenen“ Informationen

    (z.b. Liste von Hashwerten, verknüpft mit E-Mail-Adressen)

Online Angriffe

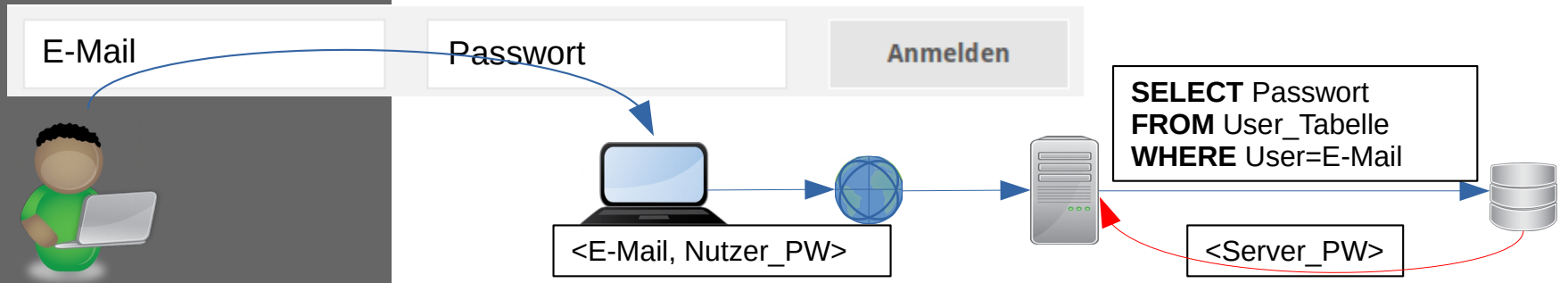
Man-in-the-middle



Online Angriffe

SQL-Injection

Eingabe



Prüfung

Theorie

Wenn
<Nutzer_PW> = <Server_PW>
Dann Loging
Sonst Fehler

Beispiel

<Nutzer_PW> = „HalloPW“
<Server_PW> = „HalloPW“

Wenn
„HalloPW“ = „HalloPW“
Dann Loging
Sonst Fehler

Angriff

<Nutzer_PW> = „TRUE OR „Bla““
<Server_PW> = „HalloPW“

Wenn
TRUE OR „Bla“ = „HalloPW“
Dann Loging
Sonst Fehler

Offline Angriffe

- Wörterbuchattacken
- Bruteforce
- Rainbow-Tables
- Hashwert-Angriffe

Definitionen

- **Wörterbuchattacken („Intelligentes Brute-Force“)**

  Wörterbuch: Liste von bekannten, oder wahrscheinlichen Passworten.
  Transformationsregeln einzelner Zeichen: Buchstaben ersetzen durch Ziffern
  (B = 8, I = 1, usw.)
  Bildung eines Hashwerts und Vergleich mit dem Hashwert des Servers

- **Funfacts**

  Der deutsche Allgemeinwortschatz umfasst 300.000 - 500.000 Wörter, der aktive sogar nur ca. 50.000 Wörter.
  Der Vorteil dieser Methode ist, dass typische Passwörter wie Namen und Geburtsdaten dadurch sehr schnell zu finden sind.

Bruteforce

- Ausprobieren aller Möglichkeiten
  - PW: 2 Stellig, Alphabet = {0 .. 9}; z.B. 78

    → Bruteforce = Raten des Ergebnisses; max 100 Versuche
  - „Intelligenter“: Zufälliges Raten

    → mind. 1 Versuch

    → max. 100 Versuche

Definitionen

- **Bruteforce (Analog zur Wörtbuchattake)**

  Keine Verwendung einer Passwortliste, Ausprobieren aller möglichen Passwörter

- **Funfacts**

  Die Länge des gewählten Passwortes ist maßgeblich für die Sicherheit. Variation der verwendeten Zeichen (Groß-/Kleinschreibung, Ziffern, Sonderzeichen) erhöht die Anzahl der Kombinationen.
  Ein herkömmlicher Hochleistungs-PC (4- Kern-CPU mit High-End Grafikkarte) kann ca. 800 Millionen Hashes pro Sekunde probieren.
  Das bedeutet, dass man bereits nach 36 Tagen alle möglichen 8-stelligen Passwörter durchprobieren kann.

Definitionen

- **Hashwert-Tabellen**

  Vorberechnung aller möglicher Hashwerte zur Passwörtern, bestimmter Länge und Zeichensätze
  Vergleich eines abgefangenen Hash-Wertes mit Einträge aus der Hashwert-Tabelle. (Nachschlagen)

- **Funfacts**

  Nachteile:

  - Hashwerttabelle kann sehr umfangreich werden
  - Eine Tabelle je Zeichensatz, Passwortlänge, Hashfunktion

  Vorteile:

  - Vergleiche sind „billiger“ als Hash-Berechnungen

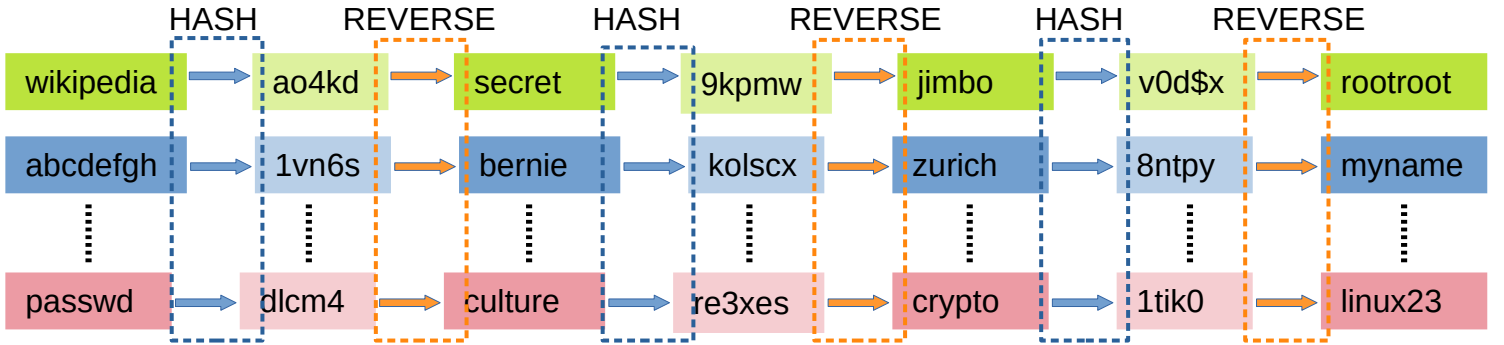
Definitionen

- **Rainbow-Tabellen (Optimierung von Hashwert-Tabellen)**

  Verkettung einzelner Hashwerten
  Speicherung von Anfang und Ende

- **Funfacts**

  Zyklen müssen vermieden werden
  Tabellen sollen „vollständig“ sein
  Vollständige Speicherung hätte enormen Speicherbedarf (TB-Bereich)



Empfehlungen (NIST / BSI)

- NIST (National Institute of Standards and Technologie)

1) Verzicht auf Komplexität:

   Pa$$w0r1!!! kaum besser als Password

2) Länge ist wichtiger: mind. 12, besser 16 oder mehr

3) Passwörter nur einmal verwenden

Länge schlägt Komplexität, Einmaligkeit ist der Goldstandard.

Empfehlungen (NIST / BSI)

4) Zwang zum regelmäßigen Wechsel kontraproduktiv: zwar sehr effektiv, aber Gefahr laufende Ziffern zu verwenden.
5) Passwortfragen gefährlich: Je nach Antwort, leicht zu eruieren
6) Passwortmanager nutzen
7) 2-Faktor-Authentifizierung
8) Sonderzeichen und Zahlen auch in PW Mitte

- Länge schlägt Komplexität, Einmaligkeit ist der Goldstandard.

1) Länge:

   Kombination mehrer Wörter

2) Erratbarkeit

   nicht zusamenhängede Worte

3) Vermeidung bekannter Phrasen

4) Vermeidung persönlicher Daten / Informationen,

   z.B. Haustiername, Geburts-Jubiläumsdaten, ...

5) Mehrfaktor-Authentifizierung nutzen

Wie kommt man nun zu einem sicheren PW?

PW Empfeh-lungen - Links

- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang_node.html;jsessionid=F31CF7FFB5DA93B32085C9BA87D14822.1_cid341
- https://www.sueddeutsche.de/digital/it-sicherheit-passwort-kennwort-tipps-passwoerter-1.3587661
- Wurde ich korrumpiert?

  https://haveibeenpwned.com/

Passwörter erstellen

- Empfehlungen
  - Länge: je Länger um so besser; mind. 12 Stellen
  - Zeichen: je mehr unterschiedliche, um so besser; mind. [0..9, a..z, A..Z]
  - Korrelation: unterschiedliche Passwörter möglichst unterschiedlich
  - Usability: nicht vergessen!!!

Ist **ji32k7au4a83** ein sicheres Passwort?

Nein!
Analogon zu „Mein Passwort“ auf der Zhuyin-Tastatur:
Zhuyin Fuhao ist eine phonetische Transkription für chinesische Schriftzeichen.

https://www.sueddeutsche.de/digital/sichere-passwoerter-ji32k7au4a83-1.4355234

Passwörter erstellen - Methoden

- Konstruieren:

  Zufällige Auswahl der benötigten Stellen

  → hohe Sicherheit

  → schlecht zu merken

- Kombinieren:

  Kombination mehrerer kürzerer Passwörter

  → schlechtere Sicherheit

  → gut zu merken

- 2-Faktor-Authentifikation: gleichzeitige Nutzung, mehrere Authentifikationswege

  → erlaubt kürzere Passwörter

  → benötigt mehrere Kommunikationswege

Passwörter verwalten

1) Berechnen:
    a) Hauptkennwort
    b) Regelwerk
2) Speichern:
    a) Gedächtnis
    b) Passwortliste (Papier, digital)
    c) Software
3) One-Time-Password
    a) 2-Faktor-Authentifikation

Passwörter berechnen

a) Hauptkennwort + Zusatz

Hauptkennwort: saoinv38fyäär1#

Zusatz: z.B. <Name Webseite>+<LoginName>

b) Regelwerk („manuelle Hashfunktion“), z.B. Passwortkarte

Auf Basis von Parametern wird das Passwort jedes Mal neu berechnet

Passwörter berechnen

b) Passwortkarte

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz.	öäü
1	43f	109	445	d.h	slk	.:7	92.	ß?e	0K.	-§s
2	9s3	+i2	ädz	âsc	ß84	sdl	49]	p}3	83y	M,6
3	32f	§r)	ört	pot	f3ü	dwz	74Ä	„d§	fl5	5Sz
4	odi	21(	+h6	d0z	&X<	O,h	jik	#&9	:6&	§so
5	apt	!äd	~42	c.2	|jh	>sd	csa	fq5	dt2	*dd
6	032	üs+	#63	,cm	1<(	Fj%	.§s	kr2	?3$	96F

Beispiel: posteo.de

Runde 1: p → .:7
Runde 2: o → ß84
Runde 3: s → 74Ä
Runde 4: t → jik
Runde 5: e → !äd
Runde 6: o → 1<(
Runde 7: . → 0K.
Runde 8: d → +i2
Runde 9: e → §r)

Passwort: posteo.de → .:7ß8474Äjik!äd1<(0K.+i2§r)

Passwörter speichern

a) Gedächtnis
   - Hohe Usability, hohe Verfügbarkeit, unzuverlässig, Nicht hackbar

b) Passwortliste
   - Papier:
     - Ausreichende Usability, variierende Verfügbarkeit, zuverlässig, nicht (digital) hackbar
   - Digital
     - Ausreichende Usability, gute Verfügbarkeit möglich, zuverlässig, hackbar

c) Software
   - Variierende Usability, gute Verfügbarkeit möglich, zuverlässig, schwer hackbar

One-Time-Password

Verlieren nach Verwendung die Gültigkeit

\+ Quasi nicht zu knacken.

− Verwaltung schwer

a) 2-Faktor-Authentifikation

- Abfrage von Zugangsdaten + Zugangscode / Einmal-Passwort
- Separate Tools notwendig (Software, Hardware, Kommunikationskanal) zur Übermittlung des Zugangscodes

b) m-TAN, photo-TAN, …

- Berechnung 1-Mal-Passwort, durch Codierung

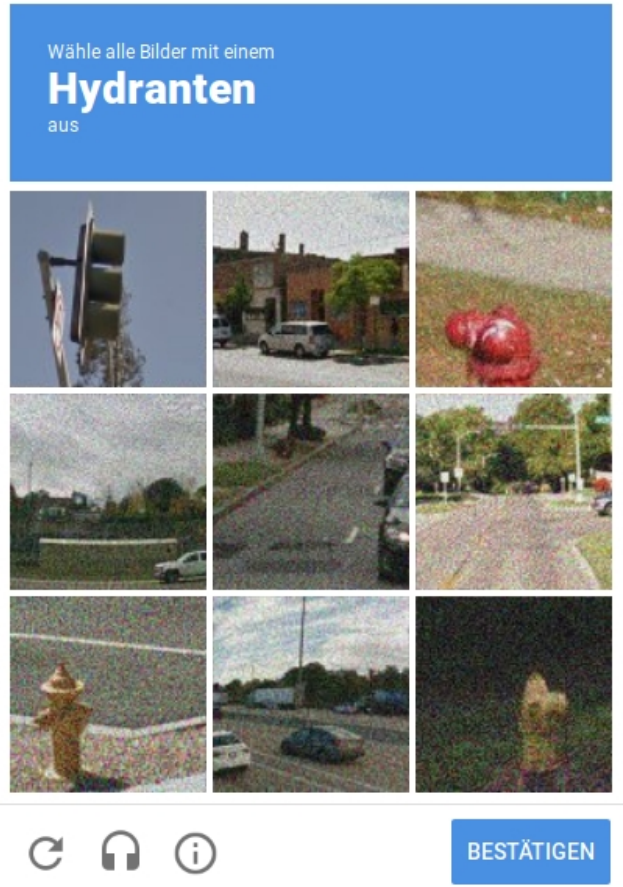
Weitere Authenti-fizierungs-methoden

- Bilderrätsel

  Beispiel: (Bild)

  möglicher Angriff:

  schwer, wegen Mustererkennung



Weitere Authenti-fizierungs-methoden

- Sicherheitsfrage

Beispiel: Wie hieß ihr erstes Haustier?

Möglicher Angriff: Onlineumfrage

- Rechnung

Beispiel: Was ergibt vier plus drei?

Möglicher Angriff: Texterkennung und KI

Sicherheit von Passwort-manage-ment Tools

Funktionsweise

- Speicherung der PW in verschlüsselter DB
- Generierung von PW regelbasiert
- Zeitlich begrenzte Zwischenablage
- Copy & Paste in Formulare
- Virtuelle Tastatur

Sicherheit von Passwort-manage-ment Tools

Tests

- https://www.netzwelt.de/passwort-manager/index.html
- https://trusted.de/passwort-manager
- (kostenpflichtig) https://www.heise.de/tests/Sechzehn-Passwortmanager-im-Test-4289884.html

- Fazit:

  Alle Passwort Manager tun was sie sollen.

  Schwächen: Zufallsgenerator

  Virtuelle Tastatur (keylogger)

  tw. Verschlüsselung und Löschen des Zwischenspeichers

In anderer Sache

Heise

- URL:

  https://www.heise.de/security/artikel/PGP-Der-langsame-Tod-des-Web-of-Trust-4467052.html

- „Titel:

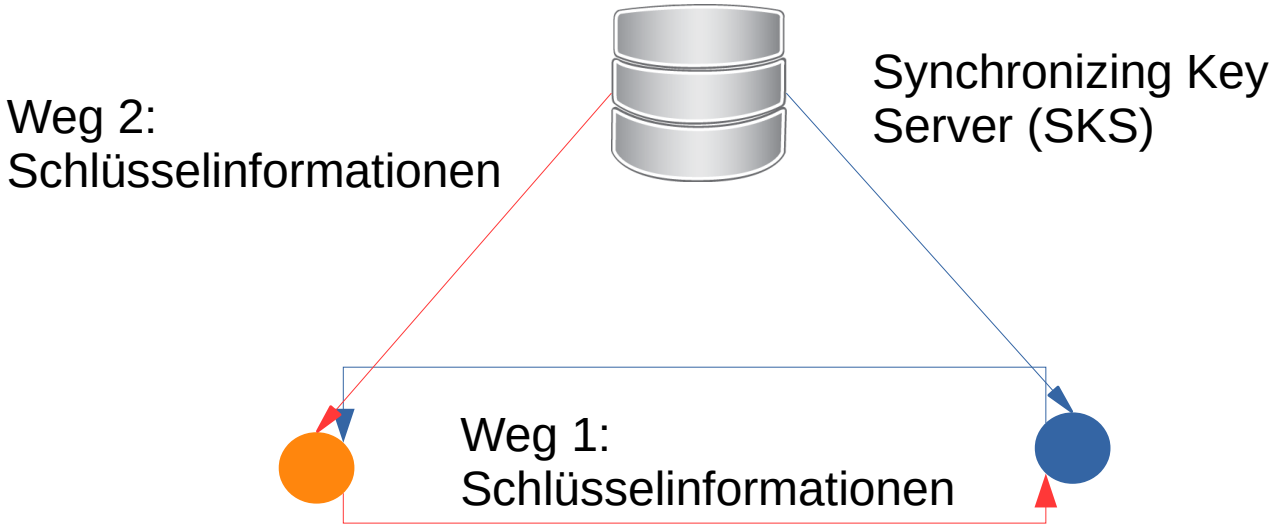
  PGP: Der langsame Tod des Web of Trust“

- Was ist damit gemeint?

  „Mit der soeben veröffentlichten Version 2.2.17 ignoriert sogar GnuPG standardmäßig alle Signaturen, die von einem Keyserver stammen.“

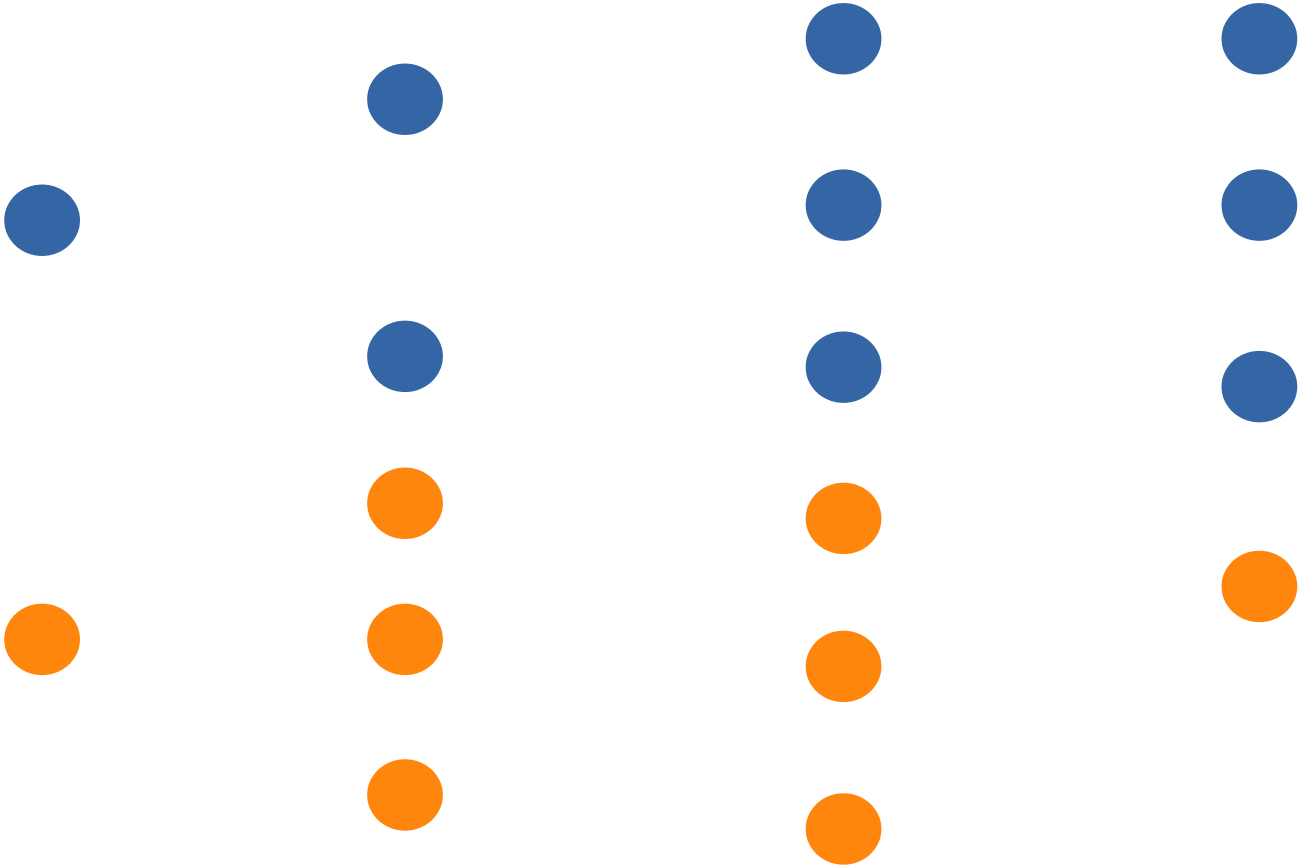
Web of Trust

Web of Trust – Signieren von Schlüsseln

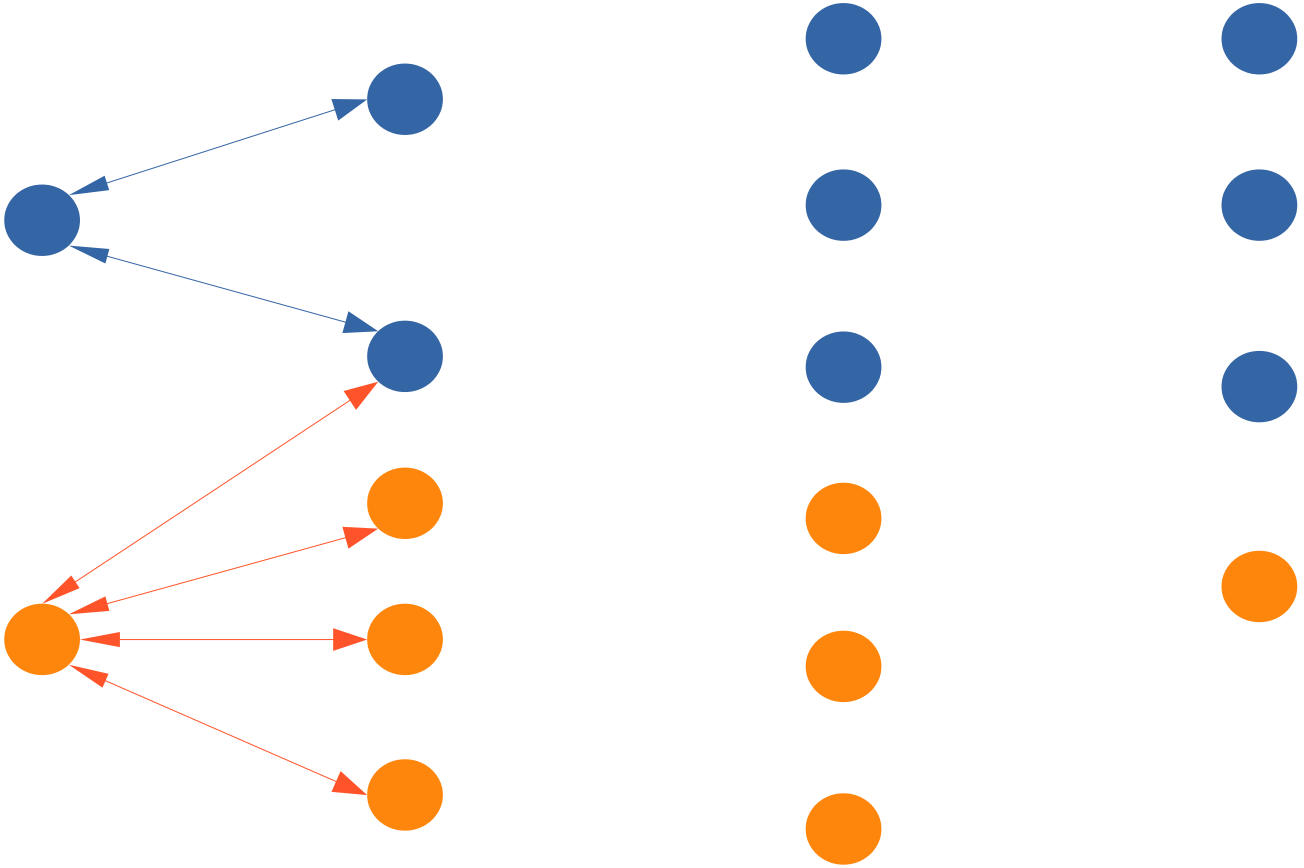


- Signieren: Bestätigung der Authentizität

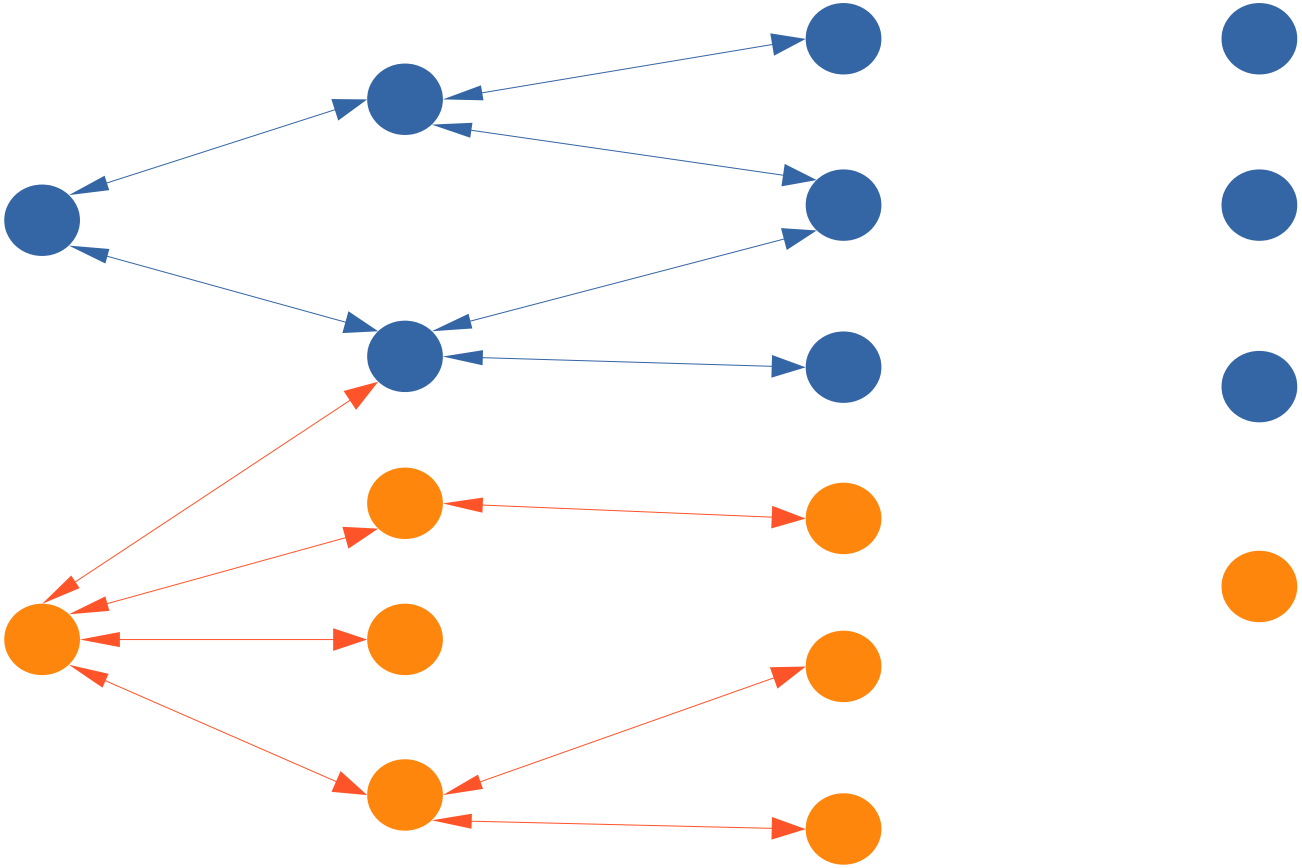
Web of Trust



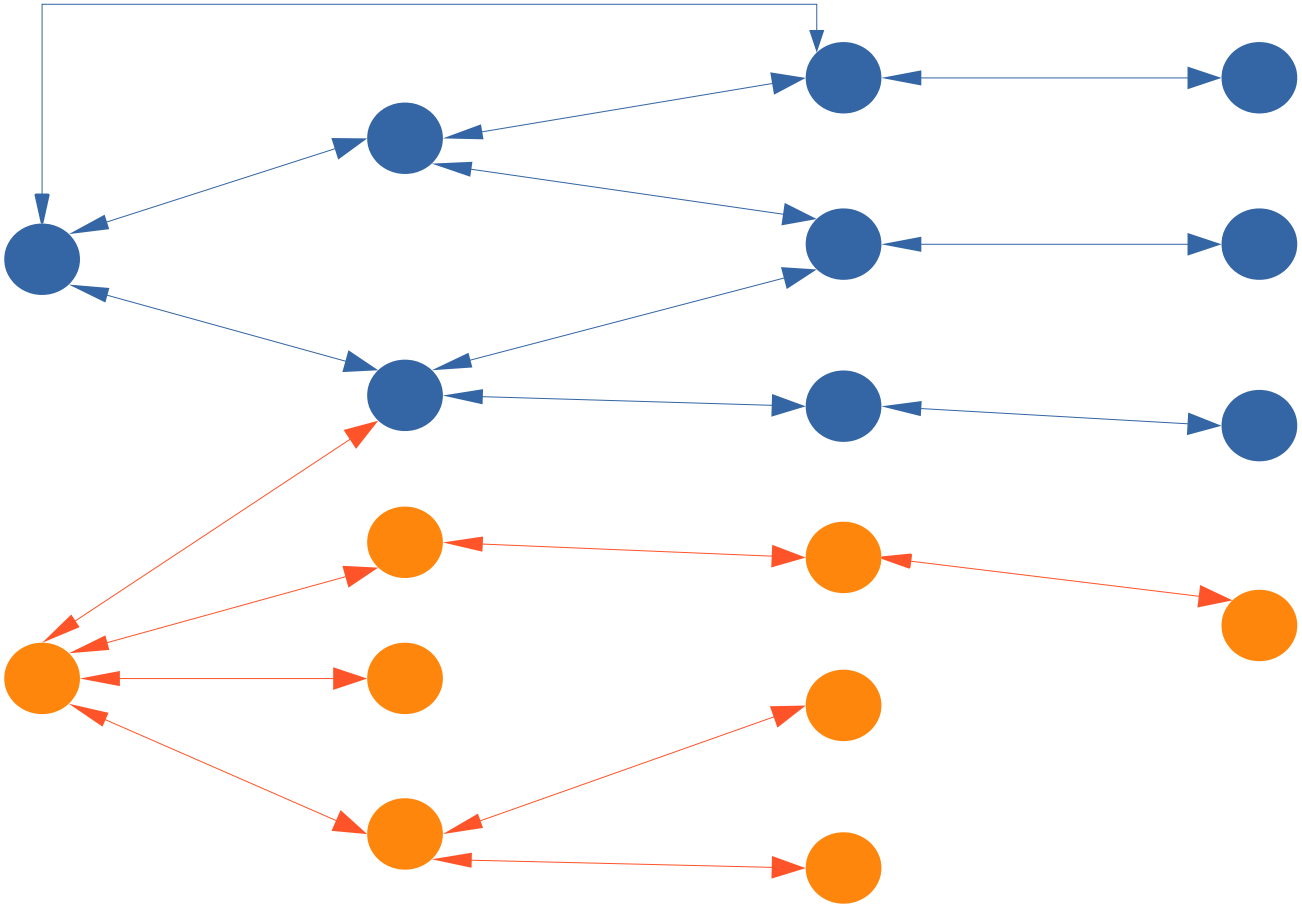
Web of Trust



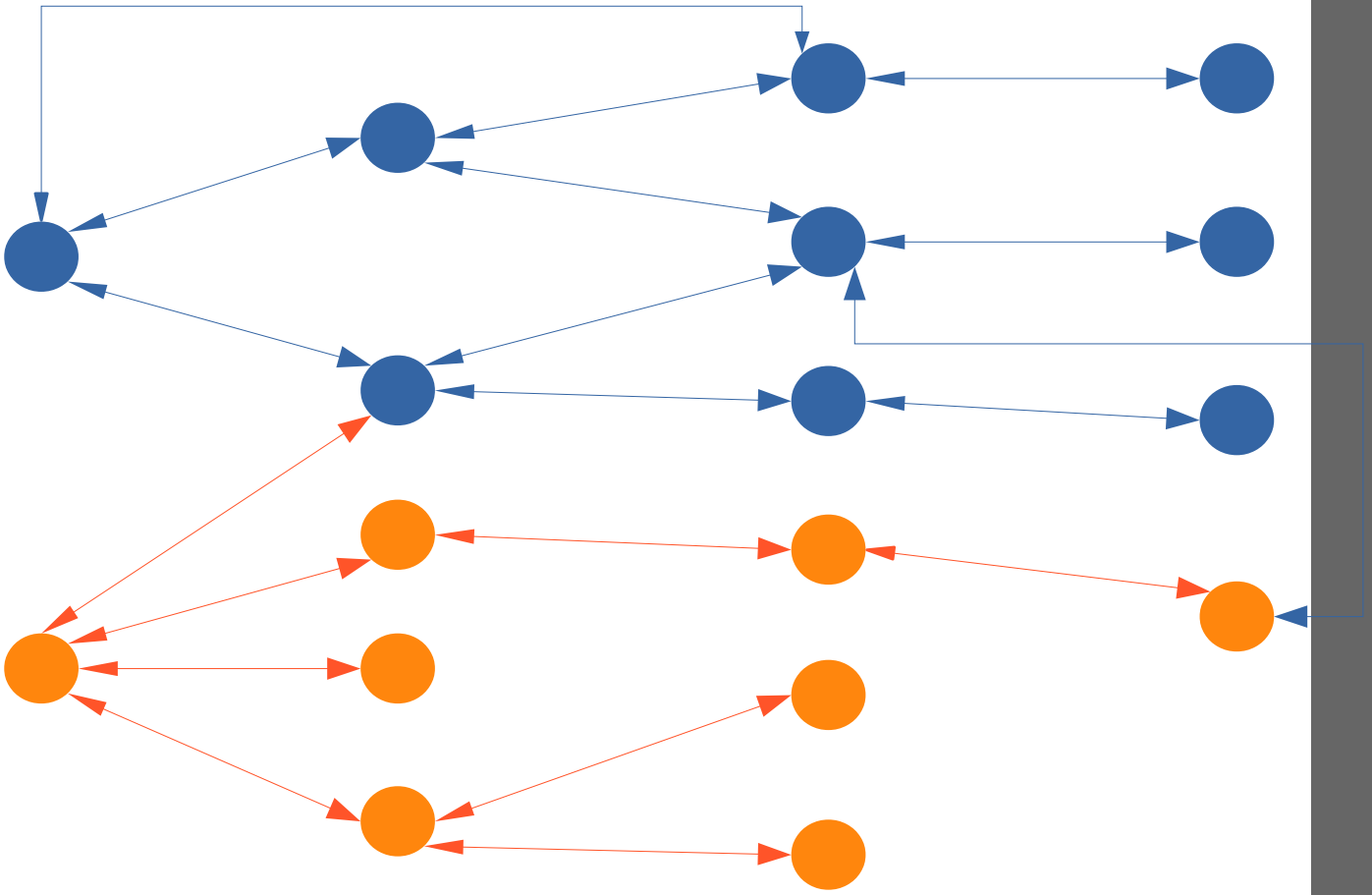
Web of Trust



Web of Trust



Web of Trust



Web of Trust