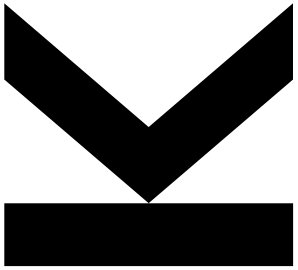
Anonym und/oder Identifiziert im Internet



JOHANNES KEPLER
UNIVERSITÄT LINZ

Michael Sonntag
Institute of Networks and Security

INSTITUTE
OF NETWORKS
AND SECURITY

Warum anonym im Internet?

- Nicht alles soll im „offiziellen Google-Profil“ aufscheinen
  - Dann bekommt man auch entsprechende Werbung…
- Manches sollte für Dritte (vorerst) unerkennbar bleiben
  - Beispiel: Undercover E-Mail an Dealer von „…@polizei.at“
  - Unternehmen: Patent-Recherchen, Übernahmen etc
  - Persönlich: Suche nach Krankheiten, Therapien usw
- Viele Dienste werden gehackt: Sie vertrauen vielleicht Facebook, aber vertrauen sich auch Cambridge Analytica und deren Kunden? Oder dem Hacker dem es gelang, Sony‘s Daten zu stehlen?
- Wer braucht schon ihre Kreditkartennummer, die Sozialversicherungsnummer & Geburtsdatum etc?
  - Damit kann man viel machen → ohne ist es sicherer
  - Keine Verbindung zur Person → schwerer nutzbar
  - Neuer Account mit ihren Daten → Geldwäsche → Indirekter Schaden (Nachweis „Das war nicht ich“ nötig)!

Anonym – Was ist nötig?

- Der Computer ist identifizierbar → IP Adresse ist zu verbergen
- Inhaltsdaten verbergen: Alles was sie identifizieren kann
  - Name, E-Mail Adresse, Physische Adresse
  - Sozialversicherungsnummer, Kreditkarte, Kundennummern
  - PLZ + Geschlecht + Geburtsdatum
  - Account-Infos: Facebook, Twitter; Telefonnummer etc
  - Metadaten in Dokumenten: Office (Computer, Benutzer), Bilder (Kamera-Seriennummer, Ortskoordinaten)…
- Wiedererkennen: „Ich weiß nicht wer es ist, aber es ist dieselbe Person wie vorher auf Website A“ + „Jetzt hat sie sich endlich angemeldet → Alles was ich vorher gesammelt habe gilt für sie“
- Kommunikationspartner: Verschlüsselte E-Mail an „headhunter@personalberatung.at“, Chat mit „drug-abuse-helpline“
- Wer ist der Angreifer: „ISP/Leitung“, „Partner“, „Computer-Dieb“?

Achtung: Dienst A ≠ Dienst B!

- Anonymes Web-Surfen funktioniert anders als anonymes Telefonieren, E-Mail versenden, Post aufgeben
  - Je nach Methode ist eine andere Anonymisierung nötig
- Was weiß der Dienst über mich?
  - WhatsApp: End2End verschlüsselte Kommunikation, aber…
    - WhatsApp weiß, wer wann wieviel Daten an wen sendet
    - Woher weiß man, wer am anderen Ende sitzt?
    - Ist das auch WhatsApp oder sieht das Programm nur so aus?
    - Habe ich das „offizielle“ WhatsApp oder eine Spezialversion nur für mich (die sich ein wenig anders verhält)?
    - Jetzt ist es sicher; aber werden die Daten trotzdem gespeichert?
    - Wie ist das lokale Backup gesichert?
- Mit anderen Worten: Erst Lernen, dann kommunizieren!
  - Es gibt leider keine Abkürzung!
  - Anonymität bedeutet Aufwand und/oder Nachteile

Beispiel: Anonymes Web-Surfen

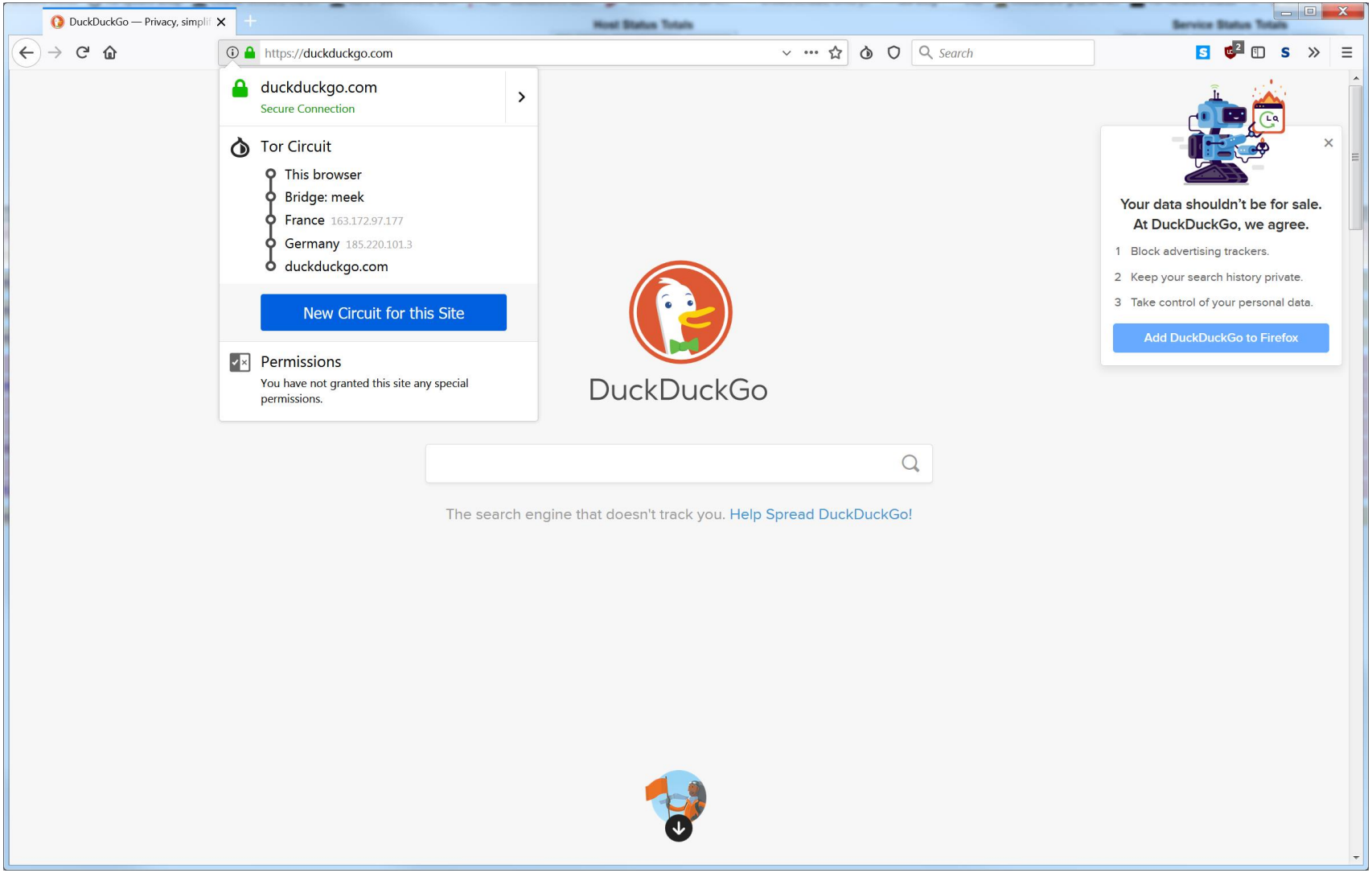
- Verbergen der IP-Adresse: Kommunikation über anderen Rechner führen, der nicht mitprotokolliert (aber: könnte; ebenso mitlesen!)
  - Zwischen-Station nötig → Langsamer; ist erst zu finden
- Inhalts-/Metadaten: Selbst zuständig; keine Hilfe möglich
  - Es gibt Tools zum Entfernen, sind aber händisch einzusetzen
  - Vorsicht beim Versenden jeglicher Dokumente!
- Wiedererkennen: „Aussehen wie alle“ und regelmäßig die Daten löschen bzw die Websites trennen
  - Trennung zwischen Tabs/Fenstern (Cookies etc)
  - Keine individuellen Daten senden, zB Bildschirmauflösung, Betriebssystem, Browser-Version, Sprachenliste…
- Kommunikationspartner: Wer die Website ist sollte man schon sicher wissen, umgekehrt braucht die Website dies nicht zu wissen
  - Zertifikate des Servers genau prüfen

Tor – The Onion Router

- Anonymisierungs-Netzwerk für Websurfen
  - Tausende Rechner auf der ganzen Welt leiten Daten weiter
  - Jede Verbindung erfolgt über drei Zwischenstationen
    - Zwei kompromittiert/loggen/überwacht → Immer noch anonym
  - Zwischenstationen werden regelmäßig gewechselt
  - Bietet eigenen Browser an (=Firefox + Modifikationen), um für alle gleich auszusehen; alle notwendigen Einstellungen erledigt
  - Zu Beginn dreifach verschlüsselt; jede Zwischenstation entfernt eine Verschlüsselungs-Schicht
    - Ergebnis: Am Ende unverschlüsseltem außer http**s**!
- Praktische Nutzung: Download → Entpacken/Installieren → Starten
  - Der Betrieb eines eigenen Knotens ist etwas komplexer
  - In Österreich legal (wurde von uns als „Muster“ durchgezogen!)
  - Hauptproblem: Bandbreite; denn Download = Upload
    - Unter 1 Mbit/s wenig sinnvoll; eher ab 10 Mbit/s

https://www.torproject.org/download/

Beispiel


DuckDuckGo — Privacy, simpli
https://duckduckgo.com
Search
duckduckgo.com
Secure Connection
Tor Circuit
This browser
Bridge: meek
France 163.172.97.177
Germany 185.220.101.3
duckduckgo.com
New Circuit for this Site
Permissions
You have not granted this site any special permissions.
DuckDuckGo
Your data shouldn't be for sale. At DuckDuckGo, we agree.
1 Block advertising trackers.
2 Keep your search history private.
3 Take control of your personal data.
Add DuckDuckGo to Firefox
The search engine that doesn't track you. Help Spread DuckDuckGo!

Exkurs: Darknet

- Darknet: Webserver, die ausschließlich über das Tor-Netzwerk erreichbar sind, zB „https://facebookcorewwwi**.onion**/“
  - Ganz normales Facebook → Niemand weiß wo sie surfen; aber keinerlei Anonymität gegenüber Facebook (Anmeldung!)
- Technischer Hintergrund: 5 Server im Tor-Netzwerk für jede Verbindung, somit weiß niemand mehr, wo der Server physisch steht
  - Nicht auffindbar, Betreiber nicht identifizierbar etc.
- Nutzen:
  - Whistleblowing, Zensur-Umgehung, Kriminelle Aktivitäten
- Identifizierung ist dennoch möglich, aber sehr schwer oder Zufall:
  - Betreiber macht Fehler → alles immer korrekt ist schwer!
  - Bestätigung vs Identifizierung: Wir vermuten wer er ist und wo der Server steht → Nachweis ist leicht!
  - Server finden & übernehmen → „Schadcode“ an Besucher senden

Passwort-Listen im Internet

- Im Internet finden sich immer wieder kleine bis riesige Listen an Passwörtern – sowohl Klartext als auch „verschlüsselt“ (gehasht)
  - Verschlüsselt: Es werden Teile/immer mehr entschlüsselt, sodass auch dies problematisch ist
- Diese Listen stammen aus Hacks
  - Eine (typischerweise) Website wird gehackt, und die Passwort-Datenbank aller registrierten Nutzer wird veröffentlicht
  - Der Benutzer kann hier gar nichts dagegen tun!
    - Es hängt ausschließlich von den Sicherheitsvorkehrungen der Site ab
  - Sowohl Hacken als auch Veröffentlichen ist illegal → Aber was nützt das, wenn die Daten einmal öffentlich sind?
    - Vergleiche ein aktuelles Urlaubsvideo aus Ibiza!
- Abgesehen davon: Es gibt Wörterbücher sowie Regeln, wie Benutzer üblicherweise/oft/gelegentlich Passwörter „konstruieren“

Konsequenzen

- Günstigste Version: Es werden nur Passwörter bekannt
  - Dann werden diese Passwörter bei irgendwelchen Nutzern bei beliebigen anderen Diensten ausprobiert
    - Praktisch: Die häufigsten Passwörter zuerst…
      - Beispeele: 123456, password, 12345678, qwerty, 123456789, 12345, 1234, 111111, 1234567, dragon
- Gefährlichere Variante: Auch Benutzername/Passwort ist enthalten
  - Dann werden gezielt diese Kombinationen getestet
  - Selbst wenn ein anderes Passwort verwendet wird: Passwort-Sperre wegen zu vieler falscher Versuche, Warn-E-Mails…
  - Gefährlicher Zusatz-Aspekt: Die Quelle weiß evtl nichts davon
    - Das Benutzerkonto gehört dann jemand anderem!
- Gefährlichste Variante: Es ist das Passwort des E-Mail Zugangs
  - Grund: „Wiederherstellung vergessener Passworte“ erfolgt meistens per E-Mail → auch alle anderen Konten sind zugänglich!

https://github.com/danielmiessler/SecLists/tree/master/Passwords

Unsichere Passwörter

- Einfache Regeln sind nutzlos: Diese sind bekannt
  - abc → d; 123 → 4; aaa → a; gZwnI → 1/2/3; Oe7b§ → Mai19; etc
- Alles was in einem Wörterbuch steht, ist gefährlich
  - Deutscher Duden: 145.000 Wörter
  - Aus deutschen Texten extrahiert: 5,3 Millionen
    - Zusammensetzungen: Donaudampfschifffahrtsgesellschaftskapitän
  - Für einen Computer sind das immer noch ganz wenige!
    - Grafikkarte (GTX 1080 Ti; bcrypt): 21.000 Hash/s, also alle Wörter des gesamten Dudens in 7 Sekunden
      - Schlechte Speicherung (MD5): 32.000 MHash/s
- Alles Passwörter mit 8 Zeichen oder kürzer
  - Man probiert einfach jede beliebige Kombination aus…
- Passwort = Benutzername/E-Mail Adresse/Website-Name/App…
- Vorname/Kosename des Partners oder Kindern, Autonummer, Name des Haustiers, Adresse, Geburtsdatum etc → Siehe Facebook!

Sichere Passwörter

- Anforderungen an PW: Länge, Komplexität, Nicht-Vorhersagbarkeit
- Wichtige organisatorische Elemente sind:
  - Sichere Passwörter
  - Passwörter für jedes Konto unterschiedlich
  - Sichere Speicherung (Konsequenz aus obigen Regeln)
- Regeln: Sinnvoll, aber oft nicht ausreichend
- Variante 1: Sehr sichere Zufallsgenerierung+Papier-Speicherung
  - Wo auch andere wichtige Papier-Zetteln sind: Geldbörse
- Variante 2: Zufallsgenerierung+Passwort-Manager
  - Man muss sich nur mehr ein sehr sicheres+ langes Passwort merken, alle anderen sind dort gespeichert (zB auch Online)
- Variante 3: Multi-Faktor-Authentifizierung
  - Zusätzlich Token oder Biometrie

Empfehlungen zu Passwörtern

- Sensibilisierung und Schulung der MitarbeiterInnen
  - Wählen des Passworts, Aufbewahrung, Weitergabeverbot…
- Speicherung im Browser → Sicheres Master-Passwort erforderlich
- Verwendung von Passwort-Managern
  - Sehr sicheres & nicht niedergeschriebenes Master-Passwort
  - Online-Synchronisation der *verschlüsselten* Passwörter
- Besonders Augenmerk auf Passwort-Wiederherstellung
  - Wie, Vorgangsweise, Identifizierung der Person
- Wenn möglich (SW-Support nötig!):
  - Umso stärker das Passwort, desto seltener ist Änderung nötig
  - Passwörter mit Listen & Wörterbüchern vergleichen und ablehnen
  - Anzeige des letzten Login-Zeitpunktes und Ortes
- Verwendung von Multi-Faktor Authentifizierung
  - Achtung: Liegt auf Schreibtisch? Daheim vergessen?

Zusammenfassung

- „Tägliches Surfen“ muss nicht anonym sein, kann es aber
  - In Einzelfällen ist Anonymität jedoch sehr wichtig; dann sollte man wissen, wie das erreichbar ist!
- Anonymität ist nicht leicht zu erreichen; der Aufwand hängt insb davon ab, gegen wen man sich schützen will:
  - Partner? Google? Detektive? Polizei? Geheimdienste?
- Eine Präsenz im Darknet ist für die meisten Firmen nicht erforderlich
- Passwörter sind weiterhin erforderlich – und weiterhin problematisch
  - Maßnahmen zur Verbesserung sollten eingeführt werden
  - Manche sind einfach (Master-PW; Passwort-Manager), andere aufwändiger (Multifaktor-Authentifizierung; Biometrie/Tokens)
  - Größter Schwächefaktor bei Passwörtern: Der Mensch!
    - Sowohl als Nutzer (einfaches Passwort), wie auch als Entwickler (Standard-Backdoor-Passwort)

JOHANNES KEPLER
UNIVERSITÄT LINZ

INSTITUTE
OF NETWORKS
AND SECURITY

https://www.ins.jku.at

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Michael Sonntag
michael.sonntag@ins.jku.at
+43 (732) 2468 - 4137
S3 235 (Science park 3, 2nd floor)

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at