Inhaltsverzeichnis

I Organisatorisches **2**

1 Einleitung **2**
1.1 Zum Kurs 3

II Internet Schlüsseltechnologien **4**

2 Internet **4**

3 IP **5**

4 DNS **5**

5 WWW **6**
5.1 Webserver 6

6 Mail **7**

7 Crypto **7**
7.1 Kryptografie 8

8 DPI **8**

9 P2P **9**

10 Werbung **9**
10.1 Probleme 10

11 Suche **10**

12 Cloud **11**

13 Social Media **11**

14 Demokratie **11**

15 CC **12**

16 Fragen **12**

III Datenschutz und Privatsphäre **13**

17 Tipps **13**

18 Fragen **14**

IV Installationsparty **15**

19 Installationsparty **17**

20 Verchlüsselung **17**

21 PGP **17**

22 OTR **17**

23 TOR **17**

24 CAcert **17**

25 Linux **17**

26 Fragen **17**

V Organisatorisches **18**

27 Fragen **18**

Teil I
Organisatorisches

1 Einleitung

Abstract

Zusammenfassung

Alles Compi zum Thema Computer, Internt, neue Medien, freie Software etc. gibt's ne Menge Fragen, die speziell Menschen in nichttechnischen Berufen, so wie wir Sozialarbeiter, nicht beantwortet bekommen, oder gar nicht erst fragen. ...

TODO: Aktuellen Abstract einfügen

1.1 Zum Kurs

Zum Kurs

Termine

Zeitpunkt	Titel
17.09.2013	Das Internet
24.09.2013	Teil 1 Forts. und Fragen
01.10.2013	Installationsparty
08.10.2013	Open Source Programme

Inhalte

- *Wie funktioniert das Internet*
- *Internet für Organisationen ?*
- *Computer, Software, Betriebssysteme ?*
- *Freie Software ?*
- *Fragen und Ausprobieren*

Teil II
Internet Schlüsseltechnologien

Aus: WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges\_wie\_das\_internet\_funktioniert.pdf`

2 Das Internet

Das Internet
Ein Netzwerk aus Computer-Netzwerken

- Netzwerk: Verbindung von Computern
- ⇒ Internet: (weltweite) Verbindung von Netzwerken
- gemeinsame Sprache: Internet Protocol (IP) *Beispiel*
- darauf aufsetzende Protokolle, z.B. SMTP, HTTP ... *von jedem definierbar, hauptsache IP (Beispiel: Adresse)*

Offenheit und Flexiblität

- einfacher Transport: Router müssen nur IP können *ISO-OSI*
- unabhängig vom Inhalt
- Innovation einfach
- schnell
- Gleichbehandlung *(?)*

3 Die IP-Adresse

Die IP-Adresse
Eine digitale Adresse

- Internet Protocol (IP)
- jedes Gerät (global) eindeutige Adresse *Spuren?*
- Ausnahmen: Privater Adressraum sowie NAT *Erklären*
- Nachverfolgung zu Geräten systemimmanent, *personenbezogene Daten?*
- Identifizierung von Personen schwer

Beispiel

172.16.254.1

4 Das Telefonbuch des Internets

Das Telefonbuch des Internets
Das Domain Name System

- Namen sind einfacher zu merken als IP-Adressen
- Adressen können sich ändern
- ⇒ DNS: Eine Art Telefonbuch *Dienst*
- hierarchisch *Durch die Instanzen, höchste: 13 „root server“*
- unsichtbar, meist vom ISP, Alternativen möglich

Beispiel
subdomain.domain.tld

5 Das World Wide Web (WWW)

Das World Wide Web (WWW)
Verlinkte Information

- HyperText Transfer Protokol (HTTP) *IP*
- Homepages in Formatierungssprache HTML (HyperText Markup Language) *Beispiel*
- offene (gemeinsame) Entwicklung *freie Nutzung, jeder kann Mitentwickeln*
- Standardisierung (W3C) *nicht jeder Hersteller eigene Sprache*

Standards

- richtige Umsetzung wichtig!!!!!!!!
- z.B. Zugang für Sehbehinderte *aka KEIN FLASH!*
- Maschinenlesbarkeit, z.B. für News-Feeds *RSS kontra Facebook*

5.1 Webserver

Webserver

- Webserver = Computer
- hat IP-Adresse und Domainnamen
- kann mehrere Domainnamen haben, viele Homepages anbieten (Shared-Hosting)

HTTPS

- Jeder auf dem Übertragungsweg kann mitlesen (Rechenzentrum bis W-Lan Zuhause)
- daher: HTTPS Verschlüsselung
- vertrauenswürdige(?) Zertifizierungsstellen *ist die Schwachstelle*
- Benutzen!!!!!!!

6 E-Mail und Sicherheit

E-Mail und Sicherheit
Post in der digitalen Gesellschaft

- SMTP
- Store and Forward *?*
- bleibt beim Zielserver oder Mailprogramm gespeichert
- ungefähr so sicher wie Postkarte: Jeder kann Absender fälschen und jeder auf dem Transportweg mitlesen/speichern/verändern *Beispiel vorbereiten! Wireshark und Telnet*

Sichere Kommunikation

- Verschlüsselung
- Signaturen / Verifikation
- Benutzen!!!!!!!
- Metadaten kaum zu verhindern *irgendwie muss der Adressat draufstehen*

7 Verschlüsselung

Verschlüsselung
Privatsphäre im öffentlichen Netz

- Vertraulichkeit herstellen?
- könnte abgefangen, gelesen, gespeichert, verändert werden
- ohne dass jemand es mitbekommt
- $\Rightarrow$ *Verschlüsselung*

7.1 Kryptografie

Kryptografie

- rasante Entwicklung folgte der Computertechnologie
- Heute: Einfache und schnelle Anwendung
- sehr schnelles(*) Knacken einfacher(*) Verfahren
- **kein Allheilmittel, keine vollkommene Sicherheit**
- muss richtig angewendet werden
- mathematisch Sicherheit nachweisbar(?)
- Verfahren: symmetrisch und assymmetrisch *erklären Beispiel/Grafik*

mögliche Angriffe

- vor/hinter der Verschlüsselung *also abfangen bevor es verschlüsselt wurde*
- z.B. Trojaner/Keylogger auf dem Rechner *Sicherheitslücken, Updates*
- z.B. auf dem Server abfangen *NSA?*
- geheimen Schlüssel besorgen *Stehlen z.B. vom Laptop am Flughafen, Firmen zwingen, Personen zwingen/foltern*
- Metadaten

8 Deep-Packet-Inspection

Deep-Packet-Inspection

Werfen wir einen Blick in ihren Internetverkehr

- Bisher: nur Paket-Header auslesen, an Empfänger zustellen
- DPI: auch Inhalt anschauen
- beides kann eine Firewall
- unerwünschte Pakete aussperren (Hacking)
- aber auch Inhalte überwachen, Werbung einblenden
- siehe China *Oppositionelle verfolgen, unerwünschte Inhalte ausfiltern*
- ⇒ Verschlüsselung

9 Peer-to-Peer

Peer-to-Peer
Von mir zu ihnen ohne jemanden dazwischen

- Bisher: Zentralisiert, Alle Clients mit (einem) Server
- P2P: Teilnehmer (Peers) sind gleichberechtigt und reden direkt untereinander
- Vorteil: kein Single-Point-of-Failure, Teilnehmer steuern Ressourcen bei. *Generell dezentral erwünscht im Internet, Ausfallsicherheit von DNS etc?*
- Nachteil: Hierarchisch ist einfacher
- Freiheit?
- wird benutzt für Videotelefonie, Filesharing, ... *Hashes, DHT, Torrent (TPB) erklären*

10 Verhaltensbasierte Werbung

Verhaltensbasierte Werbung
Jetzt wird es persönlich

- Aktivitäten von Internetnutzern aufzeichnen
- Profile erstellen
- effizientere (zugeschnittene) Werbung
- Tracking z.B. durch ID in Cookies (im Browser)

Beispiel

- Besucht eine Seite z.B. Fußball → Cookie wird erzeugt
- Besucht eine Seite über Autos → Cookie wird wiedererkannt
- Verhaltensmarketingfirma speichert das
- vergleicht mit Profilen von ähnlichen Leuten, die sich für ähnliche Dinge interessieren
- → Bierwerbung

10.1 Probleme

Probleme verhaltensbasierter Werbung

- Profiling für Strafverfolgung, Geheimdienste funktioniert genauso *man muss nur die Stichworte ersetzen: Ähnliches Vorgehen Profiling bei Strafverfolgung, oder: Interessiert sich für Islam, war dannunddann dort, → ...*
- Anonymisierte Daten zu Individuen rückverfolgbar?
- viele Daten sammeln ⇒ sehr detaillierte Profile *prinzipiell sehr genaue Vorhersagen möglich, wenn mir auch manchmal seltsame Werbung angezeigt wird*
- große Datenmengen verarbeitbar
- Google/Facebook/Amazon. Nebenerwerb von vielen Firmen
- Opt-Out *Einverständnis-Entziehungs- d.h. erstmal aufzeichnen bis gegenteiliges prinzipiell wünschenswert? Beispiel genau die Nachrichten, die mich interessieren?*

11 Die Suchmaschine

Die Suchmaschine

Ein Index für das Internet

- Internet: (Hyper-)Links, alles verlinkbar, kein zentraler Index *dezentral?*
- Suchmaschinen aka. Google
- Crawler/Spider erstellen Index *Crawlen erklären, Rafinesse und Effektivität bestimmen wie gut Suchmaschine*
- sehr komplex
- Pagerank / SEO ?
- Kommerzialisierung über Werbeeinblendungen *wobei sich der Kreis zum vorigen Kapitel schließt*

12 Cloud Computing

Cloud Computing
Das Internet wird ihr Computer

- Werbeslogan
- alles was irgendwo im Netzwerk abläuft und nicht auf dem eigenen Computer
- von jedem Gerät aus abrufbar *Kontrolle?*

13 Social Media

Social Media
Wo wir uns treffen

- Austausch nutzergenerierter Inhalte
- interaktiv
- große Nutzerzahlen u großer Einfluss
- Bsp: Wikipedia, Blogs, YouTube/Flickr, Facebook/Google+, WoW
- Probleme: Schutz der Privatsphäre, Datenschutz, Jugendschutz

14 Digitale Demokratie

Digitale Demokratie
Internet Governance

- Internet Governance
- faszinierende Möglichkeiten
- Kollaboration (siehe: Wikipedia)
- Gemeinschaftsprojekte (siehe: Debian)
- Abstimmungen?
- (alle) Informationen für jeden auf Knopfdruck
- globale Kommunikation

15 Creative Commons

Creative Commons
Mehr Nutzungsfreiheiten trotz Urheberrecht

- Dieser Teil des Vortrags basiert auf:WIE DAS INTERNET FUNKTIONIERT – Eine Anleitung für Entscheidungsträger und Interessierte `https://digitalegesellschaft.de/wp-content/uploads/2012/04/digiges\_wie\_das\_internet\_funktioniert.pdf`
- Lizenz: Creative Commons BY-SA 3.0 (Namensnennung, Weitergabe unter gleichen Bedingungen)
- Creative Commons ist eine Non-Profit Organisation
- bietet verschiedene freie Lizenzverträge an (zum Zusammenklicken)
- bieten zusätzliche Freiheiten für kreative Werke
- `www.creativecommons.de`

16 Fragen

Fragen
?

Teil III
Datenschutz und Privatsphäre

Teaser: Teil X

Teaser: Teil X

Zusammenfassung

Alle beteiligen sich Tag für Tag am allgemeinen Daten-Striptease. Und das obwohl nur wenige von uns einen Strip an der Kasse des Drogeriemarktes riskieren würden. Ob über sogenannte Rabatt- oder Kundenkarten, bargeldlosen Zahlungsverkehr oder oft nur zum Teil bewusst hinterlassenen Spuren auf der Datenautobahn.

Wir können uns bewusst entscheiden, ob wir daran teilnehmen. Beim Einkauf im Lebensmittelladen um die Ecke ist Anonymität leicht herzustellen. Doch wie funktioniert das im Internet, und wie die Voratsdatenspeicherung? Und was bedeutet es eigentlich, wenn private oder vertrauliche Daten via E-Mail quasi als elektronische Postkarte verschickt werden?

Wir möchten diskutieren und Möglichkeiten aufzeigen, wie man sich anonym, pseudonym und unter Achtung der Privatsphäre im Netz bewegen kann.

Aus: Handzettel CryptoParty (`http://procube.com/datendepot/HandzettelCryptoParty.pdf`)

Inhaltsverzeichnis

Inhaltsverzeichnis

Inhalte

- Wo und Wie Datenspuren anfallen (im Internet)
- Wer diese Daten haben will
- Wie diese Daten gesammelt werden
- Wie man verhindern kann, dass die eigenen Daten gesammelt werden

17 Tipps

So kurz wie möglich: Worauf sollte ich beim Surfen achten?

- Lange und komplizierte Passwörter: Je länger, desto weniger wirr brauchen sie zu sein. Kürzer als 12, eher 14 Zeichen sollten sie auf keinen Fall sein. Generell sollten Sie Dinge wie Telefonnummern, Geburtstage, Namen des Haustiers oder ähnliche leicht zu ratenden Daten vermeiden. Denken Sie sich am besten einen Satz aus, nehmen Sie dessen Anfangsbuchstaben und streuen Sie noch etwas Zahlen und Interpunktionszeichen ein. Literaturzitate oder Liedanfänge sollten Sie dabei auch vermeiden. Wechseln Sie Ihre Passworte häufig. Verwenden Sie möglichst viele unterschiedliche Passwörter für Ihre verschiedenen Konten. Versuchen Sie, dabei nicht wahnsinnig zu werden.

- Überlegen Sie bei Webformularen, ob Sie wirklich alle abgefragten Daten einfüllen müssen. Rechtlich müssen Sie nur die Angaben nennen, welche die Gegenseite unbedingt zur Erfüllung der gewünschten Dienstleistung braucht. Fragt ein Formular penetrant nach Ihrer Telefonnummer, ohne dass Ihnen klar ist, wozu das gut sein soll, könnte Ihnen möglicherweise eine Fehleingabe unterlaufen. Wenn Sie Ihre Mailadresse angeben sollen, aber absehen können, dass Sie nicht lang mit der Gegenseite zu tun haben wollen, verwenden Sie Wegwerf-Mailadressen.

- Verschlüsseln Sie, so oft es geht. Versuchen Sie, ob sich Seiten statt mit http: nicht auch mit https: aufrufen lassen. Das Add-On „Https Everywhere“ unterstützt Sie hierbei.

- Halten Sie Ihren Rechner und die darauf installierte Software auf dem aktuellen Stand. Auf Betriebssystemseite sollte das automatisch gehen. Für die anderen Programme gibt es unter Windows Hilfswerkzeuge, welche das Aktuellhalten erleichtern.

- Verwenden Sie unter Windows einen Virenscanner und lassen Sie die lokale Firewall eingeschaltet.

- Installieren Sie nur Software aus vertrauenswürdigen Quellen. Die neueste MS-Office-Version von irgendeiner obskuren Warez-Site ist nicht nur illegal sondern auch mit einiger Wahrscheinlichkeit verseucht.

- Vorsicht beim Öffnen von Mailanhängen. Unerwartete Zustellbescheinigungen eines Paketlieferdienstes, angebliche Softwareupdates Ihrer Bank oder wirre Rechnungen, zu denen sich weitere Informationen im Anhang befinden sollen, haben normalerweise nur ein Ziel: Sie sollen verleitet werden, den Anhang auszuführen und damit Ihr System zu verseuchen.

18 Fragen

Fragen

?

Teil IV
Installationsparty

Teaser: Teil 2

Teaser: Teil 2

Zusammenfassung

Introduce the most basic cryptography programs and the fundamental concepts of their operation to the general public. It would be nice if you know how to turn on your computer (although not required) – and bring it with you. TODO: WIFI für alle, Strom und Sitzplatz für alle, Linux-Sticks mitbringen no clear leadership Bier / Süßkram / freie Musik weitergeben der information `https://www.cryptoparty.in/organize/howto` `https://www.ak-vorrat.org/wiki/cryptoparty-erfahrungen` *(!)*

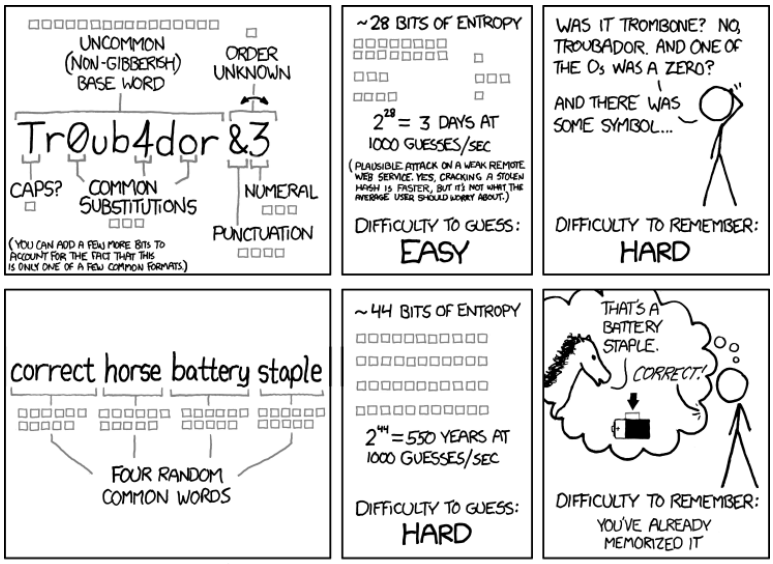
Inhaltsverzeichnis

Inhaltsverzeichnis

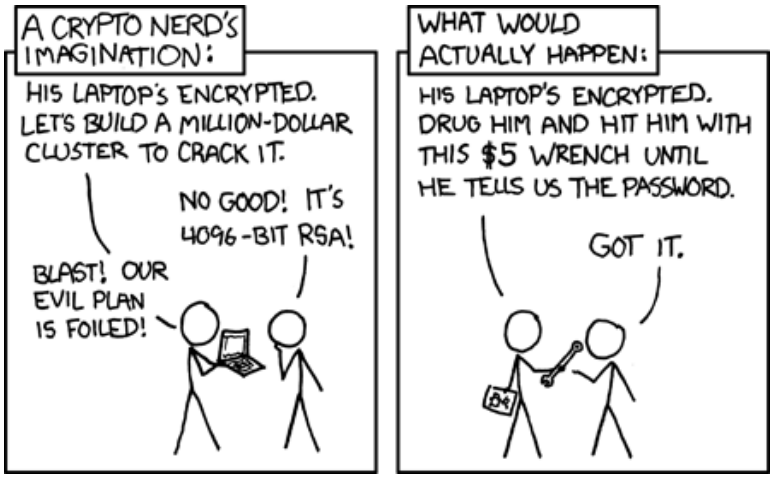
Inhalte

- Wie man seine E-Mails mit PGP oder S/MIME verschlüsselt und verschlüsselte Mails empfängt (besser noch: wie man gleich was besseres als E-Mail verwendet)
- Wie man seine Datenträger verschlüsselt
- Was ein gutes Passwort ist

Passwörter



- (CC-BY-NC) Randall Munroe `http://xkcd.com/936/`
- Password Reuse



- (CC-BY-NC) Randall Munroe `http://xkcd.com/538/`
- `https://en.wikipedia.org/wiki/Password_strength`
- `http://blog.zdf.de/hyperland/2010/11/ab_in_den_knast_fur_verschluss/`

19 Installationsparty

20 Verchlüsselung

Verschlüsselung

Die Teilnehmenden wissen/können nach der Party:

- Was asymmetrische Verschlüsselung ist und wie sie bei PGP und S/MIME zum Einsatz kommt
- was ein Diffie-Hellman Schlüsseltausch ist
- können und haben ein Schlüssel-Paar erstellt
- haben den öffentlichen Schlüssel an einen PGP Keyserver gesendet (oder lieber nicht, weil sie dort harvested werden)
- haben ihre Schlüssel-Informationen bestätigt
- Die Schlüssel-Informationen der anderen geprüft
- haben von jedem die Identität für die IDs, die sie signieren wollen, geprüft
- haben alle geprüften IDs auf den geprüften Schlüsseln signiert
- Die signierten Schlüssel an den gewählten PGP Keyserver oder an den Schlüssel-Besitzer zurückgeschickt
- machen einen Praxistest z.B. in deiner Gemeinde. (Sollte hier kein öffentlicher Schlüssel vorhanden sein, ist eine sofortige Beantragung dringend erforderlich.)

21 PGP

22 OTR

23 TOR

24 CAcert

25 Linux

26 Fragen

Fragen

?

Teil V
Organisatorisches

27 Fragen

Fragen

?