Digitale Verhütung

Thomas Keller - Chaostreff Leipzig - www.c3le.de

Überblick

- Vorstellung
- Ziel der heutigen Veranstaltung
- Es gibt keine absolute Sicherheit!
- Technisches Grundwissen

Überblick II

- Digitale Verhütung
- Fragerunde
- Praxis-Workshop

Vorstellung

Zur Person

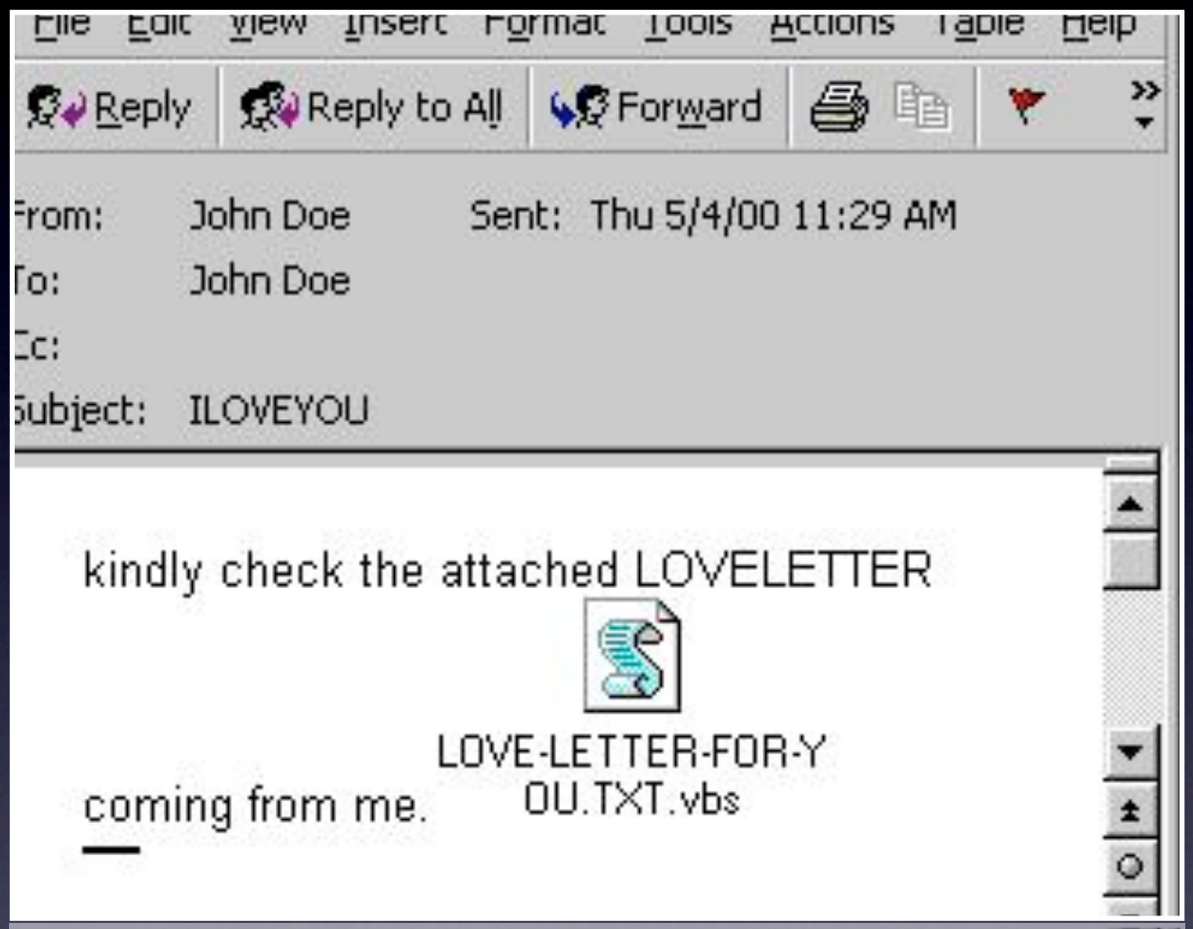
- 26 Jahre alt, verheiratet, ein kleiner Sohn
- Softwareentwickler in Leipziger Firma
- Open Source-Entwickler und Verfechter von freier Software und freiem Informationsaustausch
- aktiv im Chaostreff Leipzig und der Leipziger Ortsgruppe des Arbeitskreises Vorratsdatenspeicherung

Ziel der heutigen Veranstaltung

- Bewusstsein für Umgang mit den eigenen digitalen Daten, dem eigenen digitalen Leben schaffen
- Werkzeuge, Verhaltensweisen und Kenntnisse erlangen, um sich vor digitalen Betrügereien zu schützen
- Sicher und anonym kommunizieren

Es gibt keine absolute Sicherheit!

- moderne Kommunikationstechnologie verspricht unbegrenzte Möglichkeiten
- Nutzer gehen meist zu unbedarft mit ihren Daten um
- Anonymität wird zunehmend Luxus
- “Das größte Sicherheitsproblem sitzt meist vor dem Monitor...”



ILOVEYOU-Wurm (2000)

- E-Mail-Wurm mit „sozialer“ Komponente
- Verbreitung per E-Mail (Adressbuch) und Internet Relay Chat (IRC)
- Wurm löscht / überschreibt Dateien
- geschätzter Schaden: 5.5 Mrd USD (2000)
- u.a. geschädigte Firmen: NASA, Pentagon, Ford...

Quelle: http://www.m-boehmer.de/pdf/FROM-MANILA-WITH-LOVE.pdf

Was lernen wir daraus?

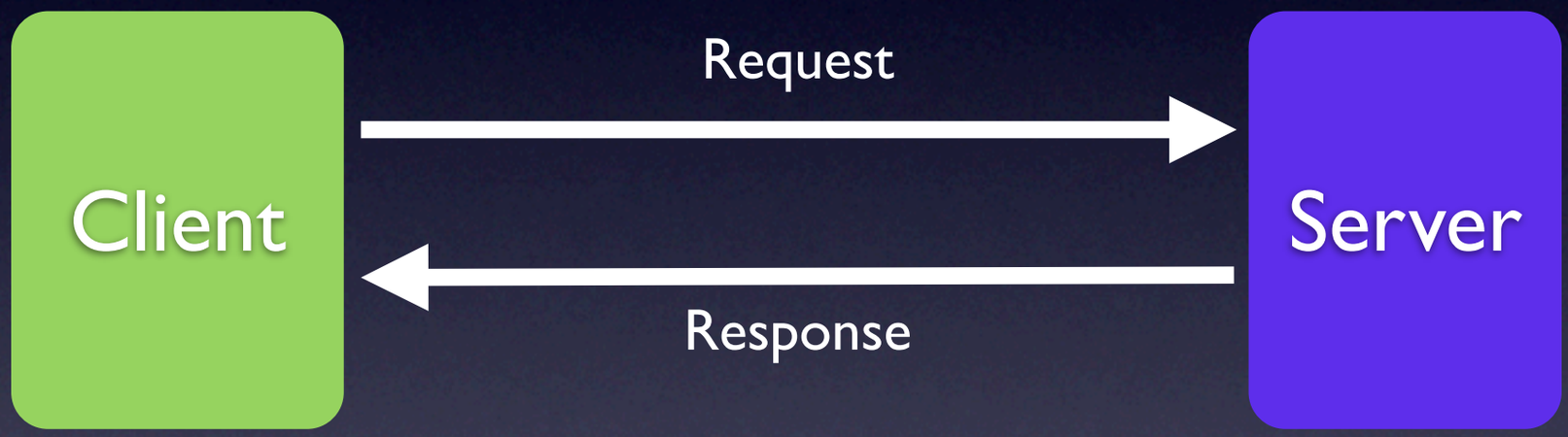
- Vertraue keinen E-Mails oder Webseiten mit fragwürdigen Inhalten!
- Wie würde man im realen Leben auf solche Angebote reagieren?
- Gesunden Menschenverstand einschalten!

Technisches Grundwissen

Client-Server-Modell

- Grundlage der meisten Kommunikations-dienste (WWW, E-Mail, FTP, ...)
- Client sendet Anfrage (Request) für einen Dienst auf einem bestimmten Port (Kanal)
- Dienst auf Server sendet Antwort (Response)
- Pull-Prinzip (wichtig!)

Client-Server-Modell



Wegfindung im Netz

- Rechner identifizieren sich über eindeutige Nummern, sogenannte IP-Adressen (IP = Internet Protocol), bspw. 209.85.135.147
- Das Domain Name System (DNS) weist den IP-Adressen (=den Rechnern) Namen zu (nicht mehr zwangsläufig eindeutig)

Was passiert beim Laden einer Webseite?

- Benutzer gibt Webadresse (bspw. www.google.de) in Browser (Client) ein
- Browser fragt nächstgelegenen DNS-Server „gib mir die IP-Adresse von www.google.de“
- DNS-Server antwortet mit „209.85.135.147“

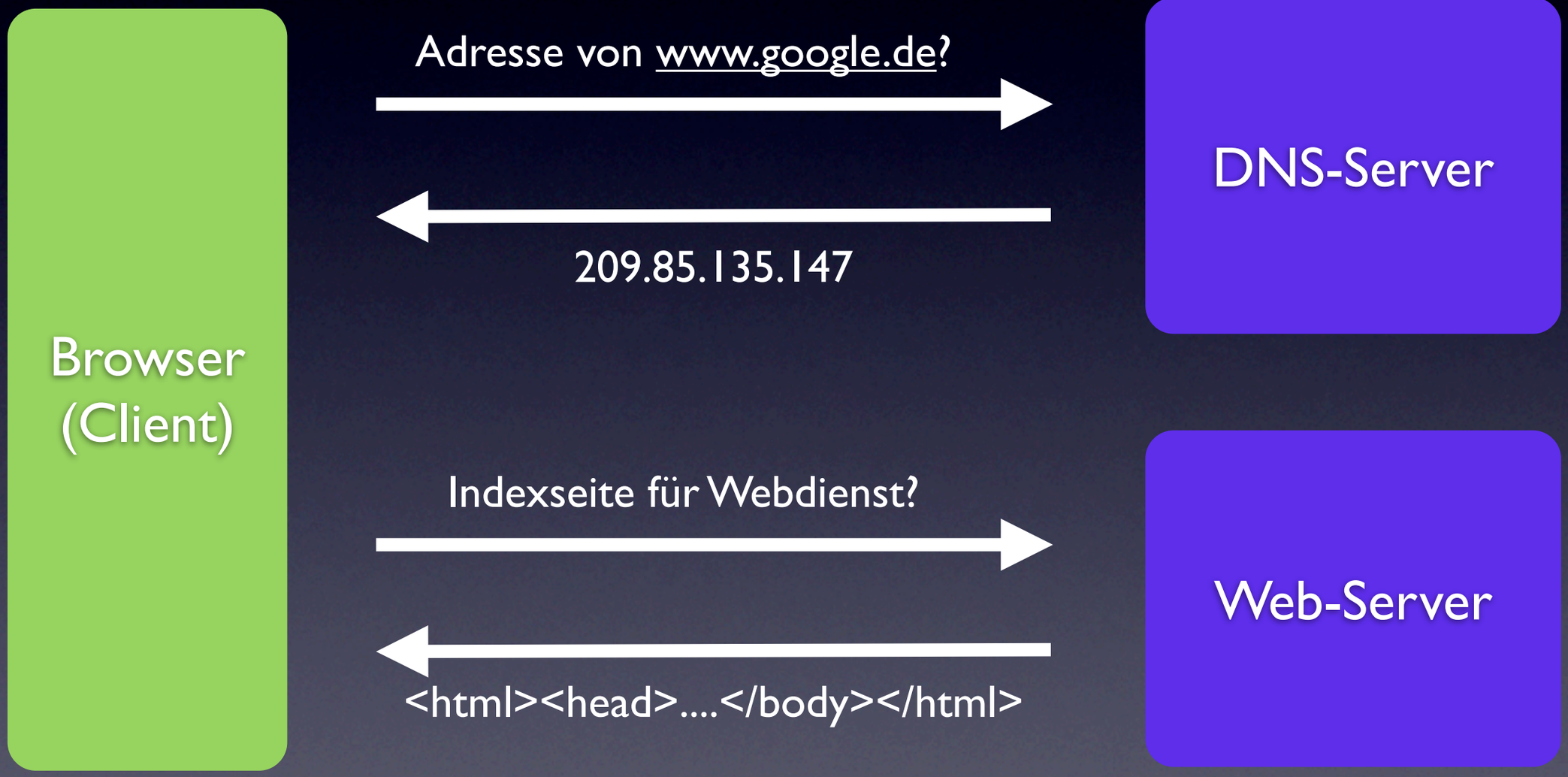
- Browser verbindet sich mit dem Rechner hinter der IP „209.85.135.147“ (Server) und dem WWW-Dienst auf Port 80

- Browser sendet in diesen Port die Anfrage „gib mir die Indexseite dieses Webservers“

- Server antwortet mit dem HTML-Text der Indexseite

- Browser stellt Webseite lokal dar

Nochmal schematisch



Und wie stehts um die Sicherheit?

- Im idealisierten Modell von eben war das nicht vorgesehen
- Über 90% der Internetkommunikation erfolgt nicht anonymisiert und ungesichert
- Eine direkte, anonyme und gesicherte Kommunikationsverbindung zwischen Client und Server ist die Ausnahme (Proxys, Router, ...)

Spurensuche

Spurensuche II

- Internetprovider merkt sich bei Einwahl IP
- Server zeichnen Verbindungsdaten auf:
  - IP-Adresse
  - Datum und Uhrzeit des Zugriffs
  - Ursprungsadresse (Referer)
  - ...

Spurensuche III

- Benutzer gibt Daten Webdiensten preis
  - Web 2.0: Blogs, Foren, Twitter
  - „Datenkraken“: Amazon, Google
- Durch geschicktes Data Mining können so Profile erstellt werden
- Das Internet vergisst nichts... schon einmal nach dem eigenen Namen gegoogelt?

Ungeschützte Kommunikation

- Rolf schreibt eine Postkarte mit Urlaubsgrüßen aus der Türkei und schickt sie an seine Oma Susi in Dresden
- Nach dem Urlaub wieder zu Hause angekommen, kümmert sich Rolf um die Abrechnung seines letzten eBay-Verkaufs und übermittelt den Höchstbietenden per E-Mail die Bankdaten seines Girokontos

Was sollte uns hier übel aufstoßen?

- Würde Rolf die Bankdaten seines Girokontos dem Höchstbietenden auch per Postkarte mitteilen...?
- Unverschlüsselte E-Mails sind wie Postkarten: Von **jedem** lesbar (Chef, Internetanbieter, Nachbar von unten)

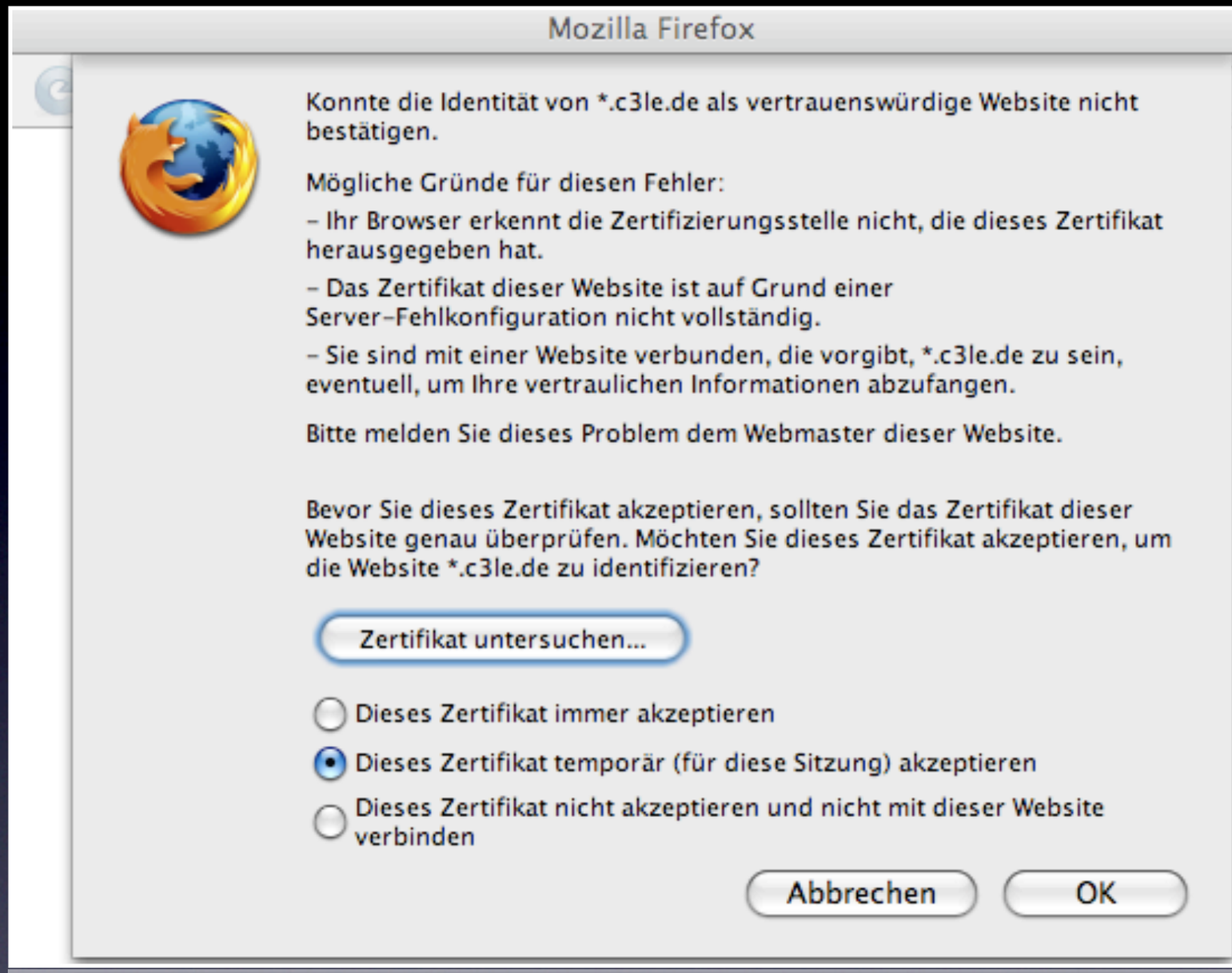
Digitale Verhütung

Sicher im Web

- Identitätsklau vor allem durch Phishing (engl. to fish = fischen) auf dem Vormarsch
- Kriminelle schicken E-Mails, die offizielle Institutionen (Banken, Versicherungen, Auktionsplattformen, etc.) vorgaukeln
- E-Mails enthalten Links auf gefälschte Webseiten, die persönliche Daten (vor allem Konto- bzw. Kreditkartendaten) „abfischen“

Wie kann man sich schützen?

- Banken, Versicherungen, etc. fordern niemals per E-Mail zur Eingabe von Logins, PINs oder TANs auf!
- Rücksprache mit der Bank halten!
- Weblink zur Bank immer über Lesezeichen!
- Auf SSL-Schutz achten...



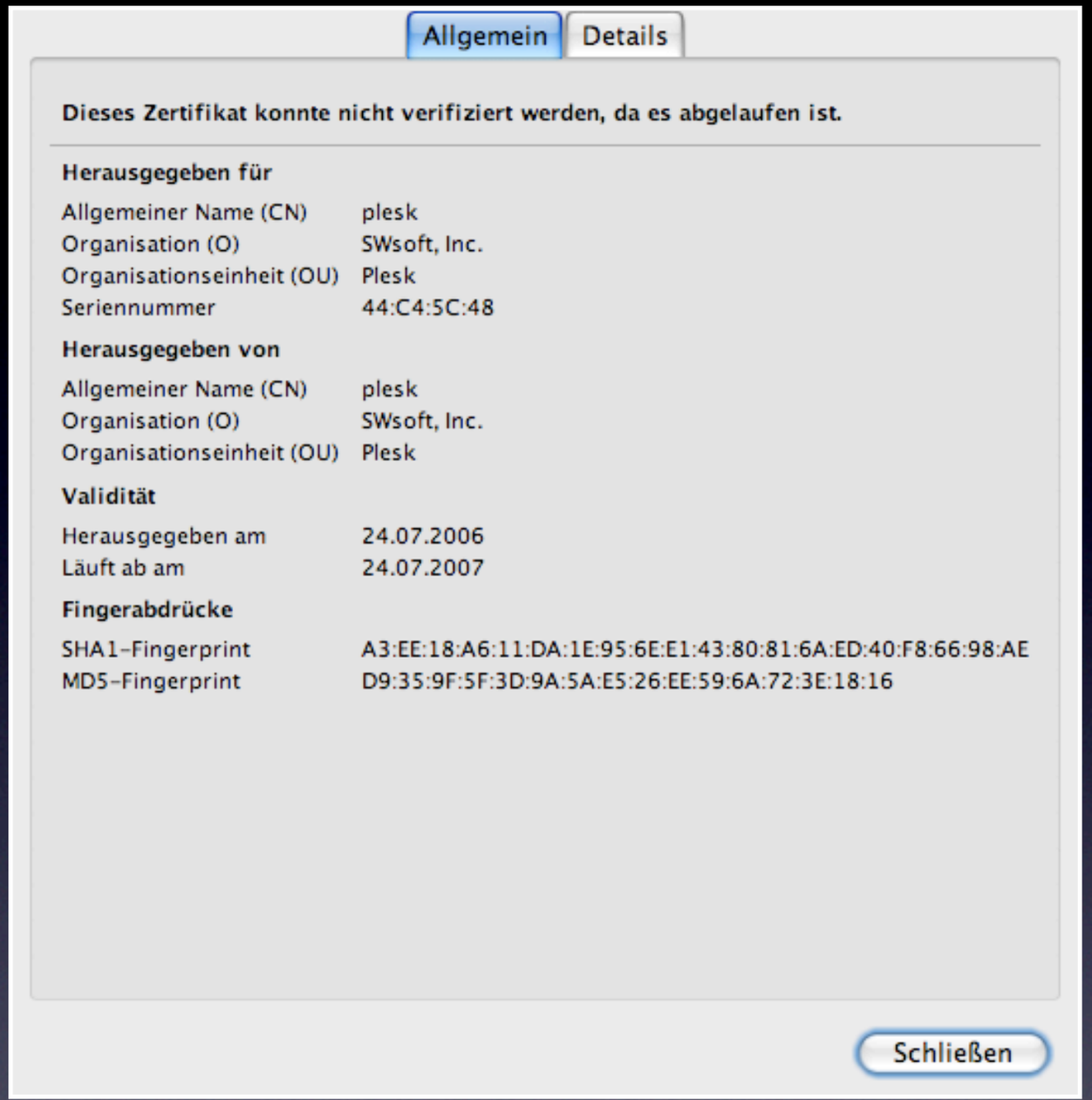
Sicherheitsabfrage im Firefox

SSL-Zertifkate

- ein SSL-Zertifikat ist ein Dokument, welches die Echtheit einer Website durch eine dritte, vertrauenswürdige Instanz bestätigt („signiert“ bzw. „unterzeichnet“)
- gültige SSL-Zertifikate werden in modernen Browsern meist durch eine gelbe bzw. grüne Adresszeile angezeigt
- ungültige / fehlerhafte Zertifikate geben Warnmeldungen aus

SSL-Zertifkate II

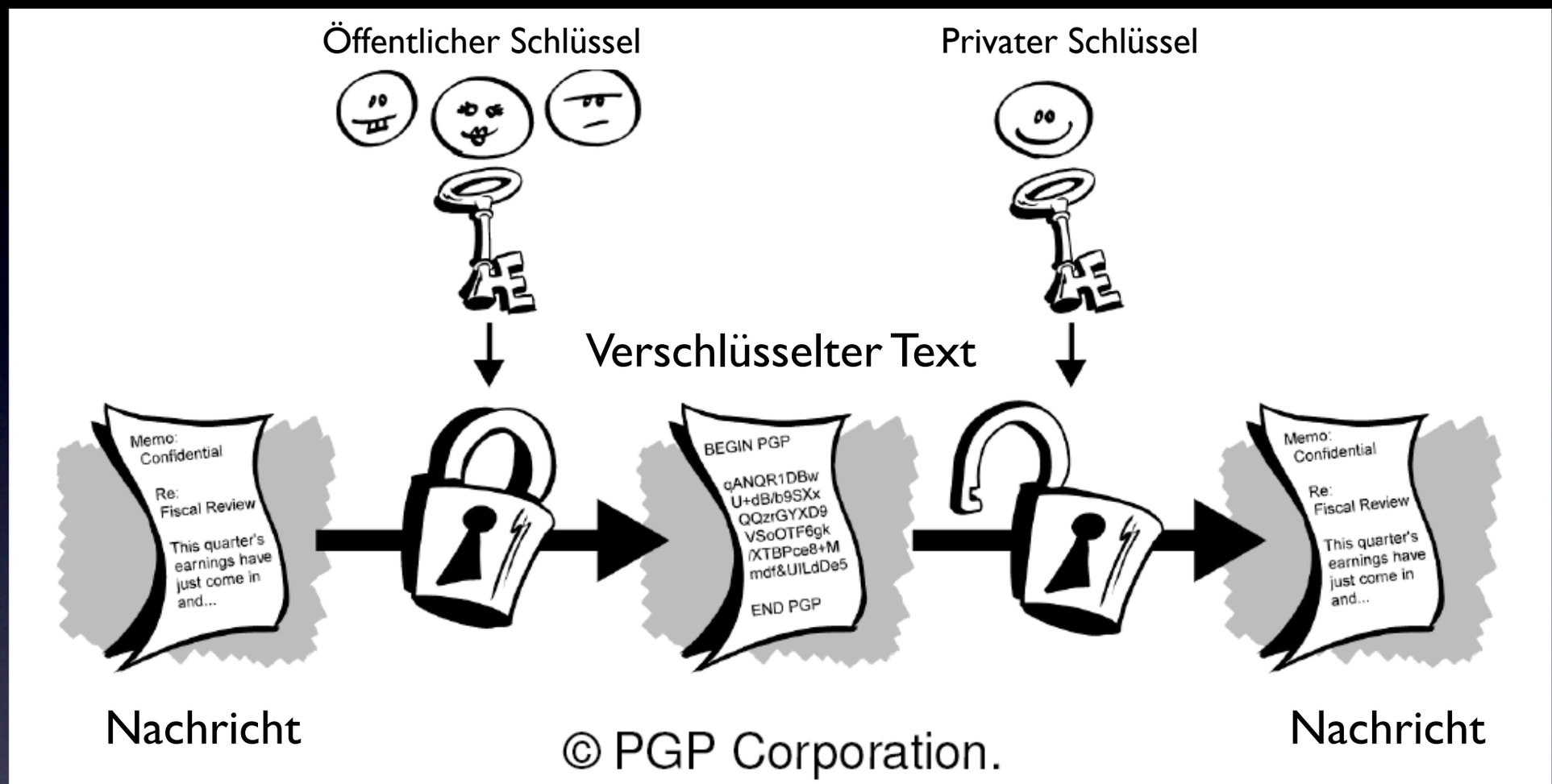
- wann ist ein Zertifkat ungültig?
  - Ablaufdatum erreicht
  - Domainnamen stimmen nicht überein
  - Instanz, die das Zertifikat unterschrieben hat, ist nicht bekannt oder nicht vertrauenswürdig...



Zertifikat-Details

Was tun gegen Mithörer / -leser?

- nicht mehr (digital) kommunizieren?
- eigene Geheimsprache (Chiffre) ausdenken, um mit meinem Gegenüber zu kommunizieren - wenig praktikabel
- Tandem aus Verschlüsselung und Anonymisierungsdiensten nutzen!

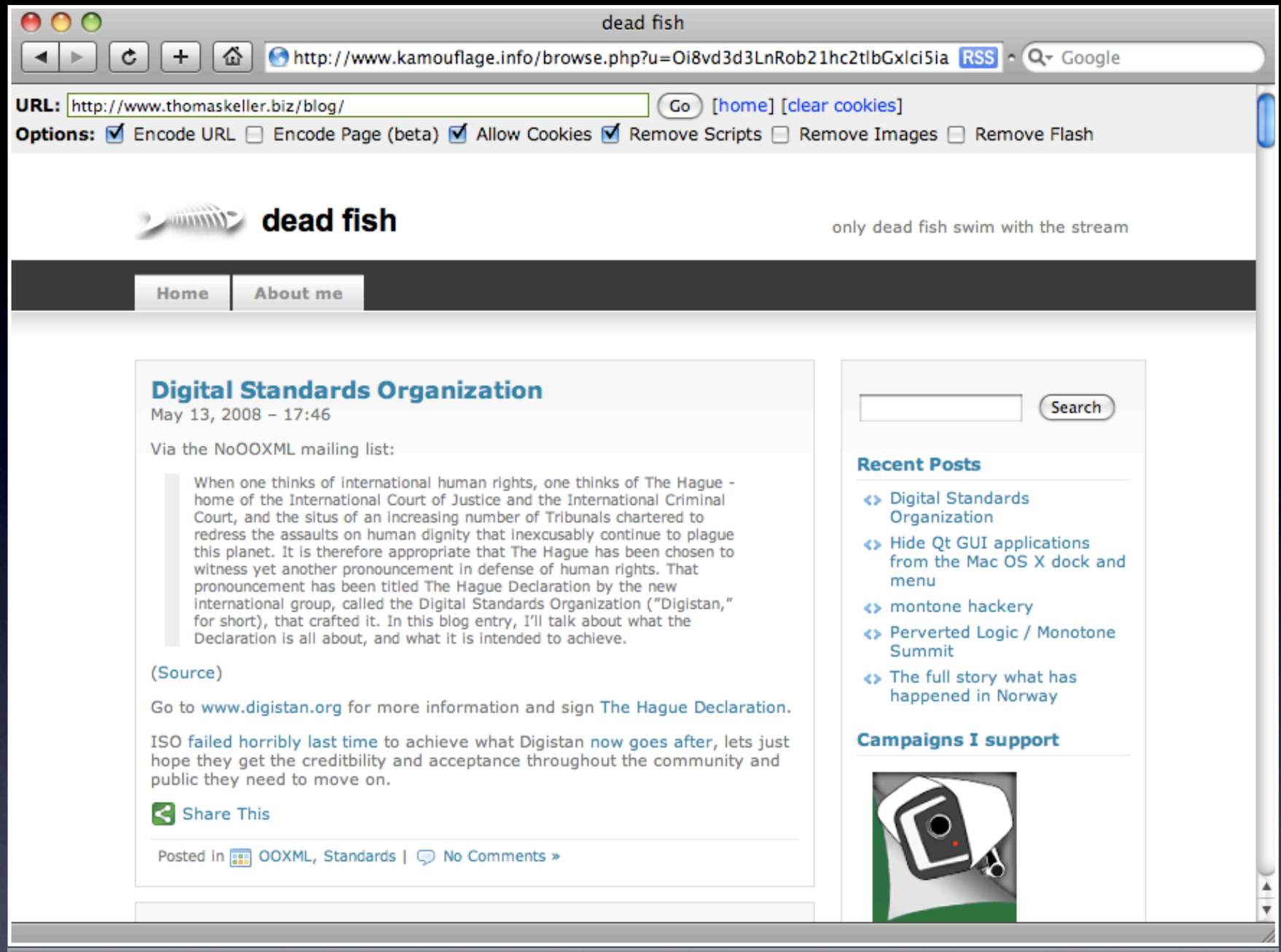


Prinzip der asymmetrischen Verschlüsselung

Prinzip der asymmetrischen Verschlüsselung

- Analogon: Briefkasten
- jeder Teilnehmer erzeugt einmalig ein Schlüsselpaar
- Schlüsselpaar besteht aus öffentlichem und privatem Schlüssel
- öffentliche Schlüssel werden untereinander ausgetauscht und authentifiziert
- privater Schlüssel wird geheimgehalten
- Anwendungen: SSL, PGP/GnuPG, u.v.a.

Quelle: http://www.christiankoch.de/c3le/2007-04-08_gnupg_druck.pdf

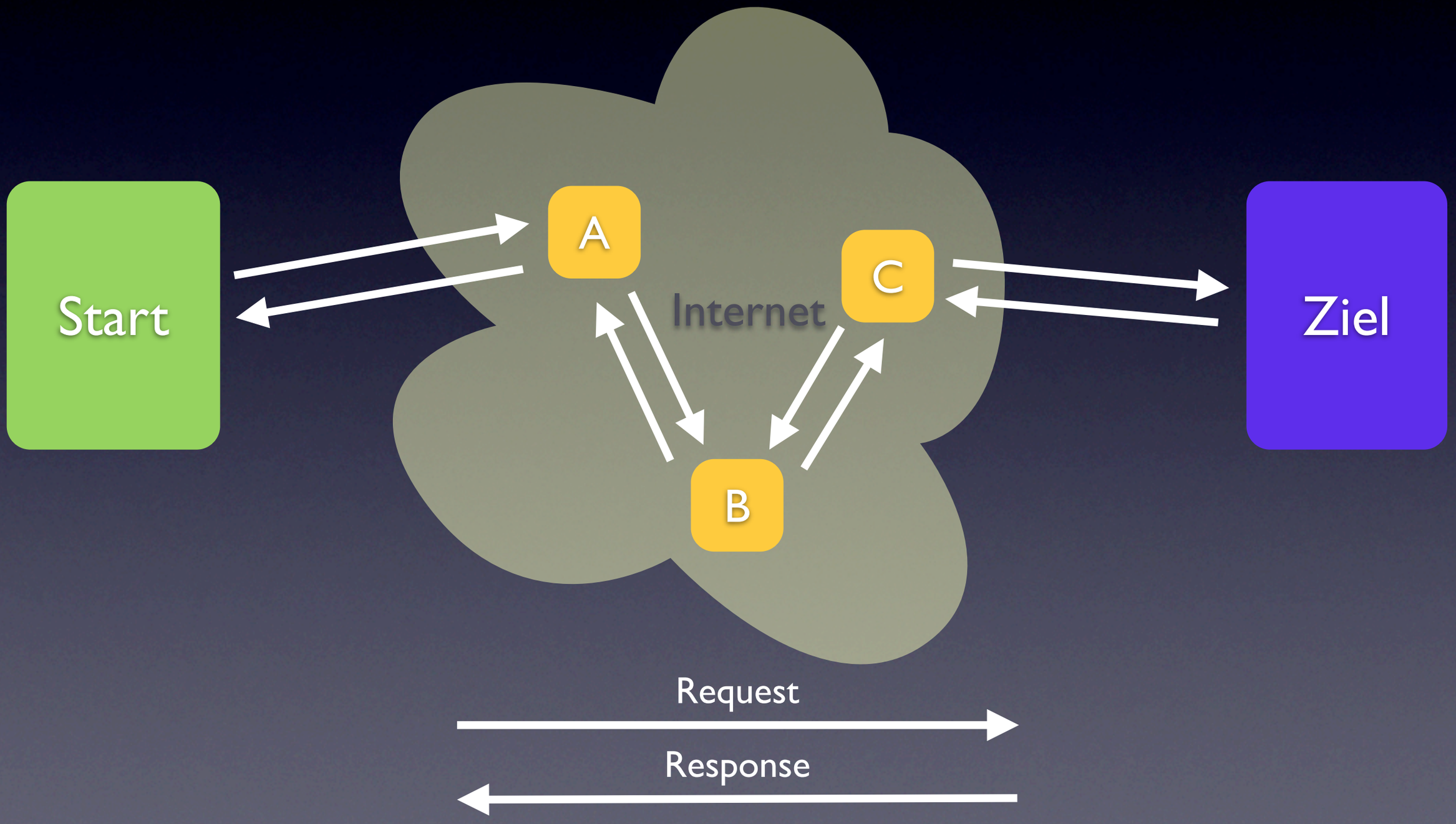


Anonymisierungsdienste

Anonymisierungsdienste

- Eben gesehen: einfacher Web-Proxy
- Aber: Problem ist nur verlagert:
  - Proxy speichert u. U. Verbindungsdaten
  - Einfache Web-Proxies nutzen normales Routing
- Deshalb: Anonymizer auf Mix-Basis...

Mix-Netzwerk



Mix-Netzwerk II

- Netzwerkverkehr wird über drei beliebige Knoten („Mixe“) A, B und C geleitet
- Zusammenhang zw. Start und Ziel aus Netzwerkstruktur nicht ablesbar:
  - A kennt nur Start und B
  - B kennt nur A und C
  - C kennt nur B und Ziel
- Übermittlung zw. den Mixen verschlüsselt

Mix-Netzwerk III

- Vorteil: maximale Anonymisierung, maximale Sicherheit
- Nachteil: langsamer Datendurchsatz (oftmals im ISDN-Bereich oder darunter), da kryptografisch aufwendig
- Anwendungen: TOR, JAP
  - Verschlüsselung des ges. Internetverkehrs
  - TOR: Plugins für Firefox und Thunderbird

Fazit

- anonyme Kommunikation ist Luxus und erfordert Anstrengungen (Konsumentzug?)
- gesundes Misstrauen ggü. fremden / „seltsam“ anmutenden Diensten ist hilfreich
- Verhältnismäßigkeit bewahren: Wer öffentliche Profile bei MySpace, XING und / oder StudiVZ hat, braucht sich keine Gedanken mehr über die Weitergabe seiner persönlichen Daten machen...

Fragerunde

Praxis-Workshop